DIGITAL FINANCIAL SERVICES (DFS) WORKING GROUP

CONSUMER EMPOWERMENT AND MARKET CONDUCT (CEMC) WORKING GROUP

GUIDELINE NOTE ON DATA PRIVACY FOR DIGITAL FINANCIAL SERVICES

Guideline Note No.43
February 2021

GUIDELINE NOTE

CONTENTS

ACKNOWLEDGMENTS

This Guideline Note is a joint product of the members of the Digital Financial Services Working Group (DFSWG) and the Consumer Empowerment and Market Conduct Working Group (CEMCWG).

Authors and contributors:
Members of the DFSWG who contributed to the Guideline Note include:

Alejandro Medina (SBS Peru), Rushika Kumaraswamy (Central Bank of Sri Lanka), Mohamed Salem Ould Mamoun (Central Bank of Mauritania), Rasool Roohy (Da Afghanistan Bank), Stephen Ambore (Central Bank of Nigeria), Anil Paul (Bank of Papua New Guinea), Khaled Barmawi (Central Bank of Jordan), Rania Elshama (Central Bank of Egypt) and Pauline Moustache (Central Bank of Seychelles).

From the AFI management unit, the project to develop the Guideline Note was led by Ali Ghiyazuddin Mohammad (Senior Policy Manager, Digital Financial Services) and supported by Eliki Boletawa (Head of Policy Programs and Regional Initiatives). We would like to thank the consultant Ros Grady for her support with relevant research and development of the Guideline Note.

We would like to thank AFI member institutions, partners and donors for generously contributing to development of this publication.

Data privacy concept. (Photo by metamorworks/Shutterstock)

EXECUTIVE SUMMARY

This Guideline Note has been developed by AFI's Digital Financial Services Working Group (DFSWG) and the Consumer Empowerment and Market Conduct Working Group (CEMCWG).

The digital financial services (DFS) market is being transformed at an exponentially fast rate, fueled by FinTech enabled data processing developments. These changes have led to innovations in the design and delivery of DFS products, which in turn help achieve financial inclusion goals and their poverty alleviation and economic growth benefits.

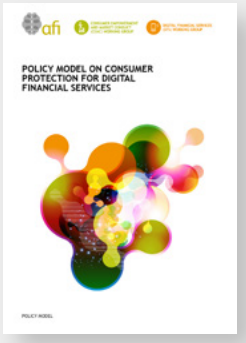
Conversely, these innovations raise significant data privacy issues for data subjects - data privacy for digital financial services (DP4DFS). Of particular concern are the likely financial capability and technology challenges of data subjects in a financial inclusion context.

The purpose of the Guideline Note is to provide non-binding guidance for a comprehensive, risk- based and proportionate policy and regulatory framework for DP4DFS. The focus is on privacy issues applicable to DFS, rather than traditional financial services. This is because most privacy issues arise in the DFS context. However, the Guideline Note may also be relevant more broadly.

The Guideline Note builds on earlier AFI knowledge products, which cover data privacy and protection issues. See especially the guiding principles relating to data privacy and protection in the AFI Policy Model on Consumer Protection for Digital Financial Services (2020) (Principle 2.1) and in the AFI Policy Framework for Responsible Digital Credit (2020) (Principle 6). Other relevant AFI Knowledge Products are mentioned elsewhere in the Guideline Note and all are listed in Annex 5.

A wide range of policy and regulatory guidance applicable to DP4DFS has been synthesized for the purposes of the Guideline Note. As well as the AFI knowledge products mentioned above, the sources considered include a diverse cross section of national regulatory frameworks and international standards, guidelines and good practices. Related research and commentary from international organizations, academics, and experts has also been considered.

FURTHER READING



AFI Policy Model on Consumer Protection for Digital Financial Services (2020) (Principle 2.1)

> View here

AFI Policy Framework for Responsible Digital Credit (2020) (Principle 6)

> View here

The result of this work has been the development of the following Guiding Principles. The Key Recommendations for each Guiding Principle are included later in this Guideline Note.

PILLAR 1: DP4DFS POLICY AND REGULATORY FRAMEWORK

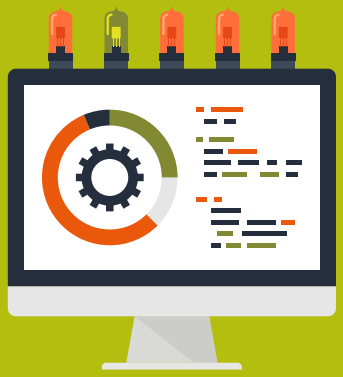
- 1.1 Guiding Principle: Establish governance and consultation arrangements
- 1.2 Guiding Principle: Assess current DFS legal and regulatory framework and market
- 1.3 Guiding Principle: Establish overarching policy and regulatory principles
- 1.4 Guiding Principle: Develop DP4DFS legal framework

PILLAR 2: DATA CONTROLLER AND PROCESSOR OBLIGATIONS

- 2.1 Guiding Principle: Require effective DP4DFS internal governance arrangements
- 2.2 Guiding Principle: Establish overarching data processing principles
- 2.3 Guiding Principle: Create model for informed and effective consent
- 2.4 Guiding Principle: Require Data Protection Officer where appropriate

SIX PILLARS OF GUIDING PRINCIPLES FOR A DP4DFS FRAMEWORK

PILLAR 1:
DP4DFS POLICY AND REGULATORY FRAMEWORK



PILLAR 2:
DATA CONTROLLER AND PROCESSOR OBLIGATIONS

PILLAR 3:
DATA SUBJECT RIGHTS

PILLAR 4:
CONSUMER AWARENESS AND RECOURSE

PILLAR 5:
SUPERVISION AND ENFORCEMENT

PILLAR 6:
DP4DFS IN GLOBAL AND NATIONAL EMERGENCIES

PILLAR 3: DATA SUBJECT RIGHTS

3.1 Guiding Principle: Establish fundamental rights of data subjects

3.2 Guiding Principle: Specify how rights may be exercised by data subjects

PILLAR 4: CONSUMER AWARENESS AND RECOURSE

4.1 Guiding Principle: Require effective internal complaints handling procedures

4.2 Guiding Principle: Provide for an external dispute resolution scheme for data subjects

4.3 Guiding Principle: Consider need for public awareness programs

PILLAR 5: SUPERVISION AND ENFORCEMENT

5.1 Guiding Principle: Take a risk-based and proportionate approach to supervision

5.2 Guiding Principle: Ensure supervisors have effective mandate, powers, capacity, and resources

5.3 Guiding Principle: Establish clear consultation and coordination framework

5.4 Guiding Principle: Consider DP4DFS issues in regulatory sandbox environments

5.5 Guiding Principle: Ensure credible threat of enforcement

PILLAR 6: DP4DFS IN GLOBAL AND NATIONAL EMERGENCIES

6.1 Guiding Principle: Provide policy guidance on application of DP4DFS in emergencies

6.2 Guiding Principle: Ensure DP4DFS legal framework makes provision for emergencies

A one-page 'Minimalist Approach to DP4DFS for Financial Sector Regulators' has also been included in this Guideline Note. This proposal contains suggestions as to the minimal actions that financial sector regulators might take in the interim period before there is a comprehensive data protection law in place.

In summary, the main body of this Guideline Note is organized as follows:

- Scope, Key Concepts and Definitions
- Emerging Trends in DP4DFS Policy and Regulatory Frameworks
- Guiding Principles for overall DP4DFS Policy and Regulatory Framework
- Minimalist Approach to DP4DFS for Financial Sector Regulators

SCOPE, KEY CONCEPTS AND DEFINITIONS

The Guiding Principles cover 'data privacy' issues affecting personal information but not issues specific to 'data protection'.

These terms are defined as follows for the purposes of this Guideline Note: 'data privacy' is considered as the appropriate use and management of personal data having regard to entitlements to privacy and 'data protection', as securing data against unauthorized use. These are the definitions used in the AFI Policy Model on Consumer Protection for Digital Financial Services (2020). On this basis, issues such as cyber fraud, security systems and data localization rules are considered to be in the 'data protection' realm. Some issues relevant to the 'grey' area that overlaps data privacy and data protection have nevertheless been covered (such as identity fraud and misuse).

For completeness it is also noted that the right to privacy is generally considered as 'the right to be let alone', albeit subject to some limitations.[1] However, it is considered beyond the scope of this Guideline Note to discuss the nature of the right to 'privacy' or whether any right or other entitlement to privacy might exist in any jurisdiction.[2]

The Guiding Principles are relevant to retail DFS products and related business models common in emerging economies from time to time (now and in the future). This could include, for example, savings, digital credit, P2P lending, e-money, remittances, micro insurance, crowd funding and investment products, as well as more innovative products and services such as account aggregation and other open banking services.

Other key issues reflected in the Guiding Principles are:

> **Financial inclusion:** The Guiding Principles are framed on the assumption that they should be relevant to consumers in economies with ambitious financial inclusion goals.

1 Sameul D Warren and Louis D. Brandeis. The Right to Privacy. Harvard Law Review Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220

2 For a discussion of these issues in the context of India see the important decision of the Supreme Court of India in Justice K.S. Puttaswamy vs. Union of India (2017) 10 SCC 1 which, in summary, held privacy to be a right protected by the Constitution of India.

- **FinTech:** The Guiding Principles have been developed considering FinTech developments that are relevant to DFS, including new and innovative providers, business models, processing systems and applications. The Guiding Principles are also intended to be 'technology-neutral', in the sense that they should be relevant regardless of the technology used to design, market, or deliver DFS.
- **Vulnerable groups:** Data privacy issues relevant to vulnerable groups are reflected in the Guiding Principles. These groups include, for example, women, youth, the elderly, persons with disabilities and displaced persons.
- **Emergencies and DP4DFS:** There are undoubted benefits in the widespread use of DFS to respond to global and national emergencies (such as COVID-19, the Ebola crisis, the Syria crisis, and natural disasters). However, there are data privacy challenges too. Against this background, a specific Pillar on DP4DFS in Global and National Emergencies has been included.

Key terms used in this Guideline Note (including the Guiding Principles) are intended to have the meanings in Annex 3. These meanings have been developed having regard to the more commonly used terms and related definitions in regulatory frameworks, research and commentary. For ease of reference, the most significant definitions are set out in Table 1 below.

It is, however, stressed that different approaches may be taken for the relevant terms and definitions, and those proposed are not intended to be mandatory.

BOX 1: DEFINITIONS OF 'PERSONAL DATA' OR SIMILAR IN DATA PRIVACY AND PROTECTION LAWS

EU's General Data Protection Regulation: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;' (section 4).

For other examples of definitions of 'personal data' or an equivalent term, see:

- Kenya's Data Protection Act 2019 (section 2),
- Malaysia's Data Protection Act 2010 (section 4),
- Philippines Data Privacy Act 2012 (section 3).

See also India's draft Personal Data Protection Bill 2019 (section 3(28)), which specifically includes any inference drawn from personal data for the purpose of profiling.

TABLE 1: KEY CONCEPTS AND DEFINITIONS

CONCEPT	DEFINITIONS
DATA SUBJECT	An individual whose personal data is or may be processed.
PERSONAL DATA	Any information or an opinion relating to an identified or identifiable individual, whether true or not, and whether kept in a material form or not, and whether automated or not.
CONTROLLER	A natural or legal entity or public authority, which alone or jointly with others determines the purpose or method of processing personal data.
PROCESSOR	A natural or legal entity or public authority, which processes personal data on behalf of the controller.
PROCESSING	Any operation conducted in relation to personal data, whether manually or automatically, including collection, use, disclosure, storage, recording, erasure or otherwise, and 'processes', 'processed' and similar words that have a similar meaning, but excluding any processing: - required for the purposes of specified activities (such as a judicial function, enforcement of a claim, national security or a purely domestic or household purpose); or - undertaken for a purpose required or permitted by law

BACKGROUND AND CONTEXT

NEW FORMS OF DATA PROCESSING, FINTECHS AND DP4DFS

The 'Big Data' phenomenon and related technologies are fueling DFS innovations and opportunities, including in developing countries.

'Big Data' for the purposes of this Guideline Note may be considered as massive, complex data sets that are characterized by huge volumes of traditional and alternative forms of structured or unstructured personal data, with enormous variety that can be processed at great velocity for the purposes of DFS.

The categories of data which can be processed include: both traditional forms of client, account and transaction data, and alternative forms of data such as social media data, data derived from mobile phones and publicly available data. Increased internet connectivity and smart phone adoption may also provide a rich source of data for processing and increases the availability of DFS.[3] Relevant technologies include algorithms, which facilitate machine learning, cloud computing, blockchain technology, biometric identification tools and digital ID systems.[4] Finally, these new forms of data processing can be used:

- To re-identify a person by matching anonymous data (de-identified data) with publicly available data, already known information or other data; and
- To infer sensitive data from non-sensitive data (such as using a person's name to infer their race or religion or gender).[5]

FinTech entities relying on these developments are different from traditional financial service providers. It is no longer the case that data is processed for DFS purposes by highly regulated entities, such as traditional banks, insurers or securities entities, which are subject to market conduct as well as prudential rules. An ever-increasing range of new, innovative, nimble, and often borderless, FinTech entities and business models, are now processing the data either as the actual financial service provider or as a third-party service provider (such as for the purposes of data analytics).

BENEFITS OF NEW FORMS OF DATA PROCESSING

The data processing developments described above may create significant benefits for DFS data subjects. Brief examples include:

- **Product choice:** Consumers are likely to have greater access to a wide range of financial services, including nano credit products for those without formal credit histories; peer to peer lending products; payments products such as e-money; micro insurance products; low-cost savings accounts; and crowd funding. Further, open banking services such as account aggregation can provide data subjects with enhanced control over their data and related benefits in product choice and pricing, and management of their financial affairs.
- **Personalized products:** The vast amounts of personal data available to DFS providers can be used to design and offer products, which are specific to the needs and risk profile of data subjects and can be priced accordingly.
- **Easier identification:** Digital ID systems developed in reliance on new sources of data, such as biometric data and enhanced processing technologies, can facilitate secure access to DFS.
- **Emergency relief:** Identification of recipients entitled to emergency relief (such as Government to Person (G2P) cash transfers and subsidized credit) can be facilitated.

DFS providers are likely to be advantaged by these data processing developments. They may enhance their ability to design, market and price targeted financial products and services and to manage data - related business risks (such as credit risks, insurance assessment risks and complaints and claims). Some providers may also seek to sell access rights to third parties. Realization of these potential advantages would, of course, be subject to applicable laws.

Data processing developments also have a range of potential benefits at the country level. In summary, in the DFS context, this could include assistance in reaching financial inclusion goals; in developing and managing national ID systems; in encouraging competition and innovation in the financial sector; and in managing risks in the financial sector.

3 GSMA: State of Mobile Internet Connectivity Report (2020)

4 World Bank: Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting (2018)

5 ITU: Financial Inclusion Global Initiative (FIGI) Security Infrastructure and Trust Working Group, Big data, machine learning, consumer protection and privacy (2018)

RISKS WITH NEW FORMS OF DATA PROCESSING

BOX 2: AFI POLICY MODEL ON CONSUMER PROTECTION FOR DIGITAL FINANCIAL SERVICES (2020)

"In the digital financial era, data is at the core of DFS.

…

In this context, inappropriate use, management and storage of clients' data coupled with poor disclosure and transparency, has the potential to exclude vulnerable segments from financial services, drive a lack of trust in DFS and erode the gains in financial inclusion" (Guiding Principle 2.1: Safeguarding Privacy and Protection of Personal Data).

There are a wide range of risks for DFS data subjects with these developments, especially where there is not a data privacy regulatory framework in place. At a high level, these risks may result in harmful consequences such as denial of a DFS or a government benefit, financial loss, social or professional reputation damage, or unfair treatment such as discrimination. More specifically, they include the following significant risks:

- **Data subjects may have no or limited control over their personal data**: No or limited information may be provided or available about what types of data are being processed, by who, how or where. Even where information is available, consent may not be freely given or informed.
- **Sensitive data may be compromised through unauthorized collection, use or disclosure:** There are heightened concerns with the privacy of data which may be considered especially sensitive. For example, information about a person's biometric data, official identifier, religious or political beliefs or affiliation, race, ethnicity, caste, health, or sexual identity. Further, as noted above, non-sensitive data may be used to infer sensitive data.[6]
- **Incorrect, misleading, incomplete, or out of date personal data may be processed:** This may lead to unfair treatment, such as an unjustifiable denial of a credit facility, debtor harassment, an unfair refusal of an insurance claim or denial of government benefits, as well as financial losses and reputation damage.
- **Automated decision making, including profiling may lead to unfair decisions:** Decisions about a data subject, which are made on the basis of automated processing and profiling without any human intervention may result in discrimination and unfair biases.[7] Further, data subjects are not likely to understand complex, constantly evolving algorithms and other technologies used in such processes. An added complexity is that these technologies may be considered to be commercially confidential and may be protected by intellectual property rights and obligations.
- **Identify fraud and misuse of digital IDs may occur:** These events may result in financial loss and reputation damage for data subjects. There is also the added complexity that compromised biometric identity data cannot be corrected, unlike other compromised security credentials (such as a password or personal identification number). See further in section headed, 'Digital IDs and risks of Identity fraud, misuse, and inappropriate access'.
- **Recourse rights may be limited:** Without a data privacy regulatory framework in place, the data subject may have no recourse for any misuse of their data. This could include, for example, recourse that requires the data controller to stop or change their processing of the personal data or to correct or delete any records they have or to pay compensation.
- **Data controller systems and procedures do not ensure privacy:** There may also be a risk that data controllers do not have in place overall systems and procedures that proactively reflect privacy considerations in the design and marketing of DFS. To put it another way, privacy issues are not at the 'forefront'. This may be more likely with new, innovative FinTech entities, as compared to more traditional DFS providers.
- **Privacy risks with intermediaries such as data brokers who trade in Big Data and the related analytics are coming under increasing scrutiny:** For example, the UK Information Commissioner's Office recently investigated 3 credit reference agencies who also operated as data brokers.[8]

DFS providers may also be challenged by new data processing developments, even without obligations to comply with a data privacy regulatory framework.

6 India's draft Data Protection Bill (2019) (Section 3(36))

7 G20: High-Level Principles for Digital Financial Inclusion (2016) (Principle 5 refers to as a key action to support DFS: 'Require that data not be used in an unfair discriminatory manner to digital financial services (e.g., to discriminate against women in relation to access to credit or insurance)'.

8 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/

They include: the complexities and costs involved in keeping up-to-date with these innovations and adjusting existing systems and processes; the business implications of processing inaccurate or irrelevant data; the resulting need for more complex data collection and verification methods; the risks and costs with increased dependance on external providers of data and data analytics, and the need to build customer awareness of the need to safeguard their personal data, official IDs and security credentials.

There are also challenges for financial sector regulators and policymakers in the DP4DFS context. In general terms, they include the potential for consumers not to trust the use of DFS because of concerns about data privacy, with implications for financial inclusion. More specific challenges may be the need for regulators and policymakers:

- To understand the business models, partnerships, activities, and data processing techniques of new, nimble, and innovative FinTech providers;
- To acquire appropriate organizational and technological capacity and resources;
- To understand any gaps and overlaps in sector - specific DP4DFS rules (e.g., in banking, payments, e-money, or general consumer protection laws); and
- To establish consultation and coordination arrangements with other government agencies, the private sector (including both traditional and FinTech DFS providers) and civil society stakeholders (such as consumer groups).

DP4DFS AND VULNERABLE GROUPS

Vulnerable groups need to be considered in developing a DP4DFS regulatory and policy framework. As mentioned above the term 'vulnerable groups' covers data subjects who are likely to have special needs including women, youth, the elderly, persons with disabilities and displaced persons. Issues of special concern include:

- **Women:** Cultural norms in some societies may mean women are especially concerned about the privacy of their DFS data, including as far as other household members (such as their partners) and their communities are concerned.
- **Youth:** Young people are likely to have grown up with a familiarity of FinTech-enabled technologies and DFS, although it is not clear that they understand all the related privacy risks.
- **The elderly:** This group is especially likely to suffer from limited financial and technological capabilities, which may in turn disproportionately affect their ability to understand and exercise any data privacy rights.
- **Persons with disabilities:** There is a wide range of disabilities, which may be relevant to reading or understanding data privacy disclosures and forms of consent. They include visual and intellectual disabilities, as well as language limitations. The latter point is especially likely in countries that have multiple official languages and local dialects.
- **Displaced persons:** Data privacy issues for this especially vulnerable group may include concerns about who has access to their personal data, including biometric records created by relief organizations such as UNHCR (for example, to facilitate delivery of cash assistance through DFS). This issue is widely discussed, including by UNHCR, which has its own Data Protection Policy.

The above factors suggest a need to look at the diversified range of DFS users when developing a DP4DFS policy and regulatory framework, and to develop targeted literacy programs.

BOX 3: SPEECH BY AFI EXECUTIVE DIRECTOR DR. ALFRED HANNIG (NOVEMBER 18. 2020)

'"Digital literacy plays an important role as users to learn to navigate these services. There should be focus and proportionality to what the regulators can do in educating financial customers, especially those that are nor familiar with the risks. For example, the elderly are not used to the DFS and internet banking, and due to their lack of knowledge, face risks of falling out of the system. Therefore, regulators need to look at the diversity of groups and risks they face."

Low-income financial services customers have shown that they care about data privacy. There are various surveys and studies to support this view, although some indicate consumers may be prepared to share data with financial firms for additional benefits.[9] More specifically, recent experiments by CGAP in Kenya and India found (in summary) that most of the participating poor customers:

- Value data privacy and are prepared to pay for it through a higher fee or interest rate;
- Were prepared to spend time in obtaining a loan that offers privacy; and /or
- Were unwilling to share personal data with third parties.[10]

DP4DFS AND FINANCIAL INCLUSION

Is there a trade-off between financial inclusion and data privacy rules? It may, for example, be considered that data privacy rules inhibit DFS innovations such as digital credit and micro insurance products or impose restraints on open banking services or the use of certain technologies such as cloud computing services.[11] The contrary view is that data privacy and financial inclusion are compatible goals, as data privacy rights are likely to build trust in the use of DFS. Further, a proportionate data privacy regime may provide a foundation for innovations such as open banking facilities and economic digitization, generally.[12] Unregulated data practices may also work against the fundamental goals of financial inclusion (see Box 4).

BOX 4: DR KATHERINE KEMP, SENIOR LECTURER, UNIVERSITY OF NEW SOUTH WALES: 'BIG DATA, FINANCIAL INCLUSION AND PRIVACY FOR THE POOR' RESPONSIBLE FINANCE FORUM (2017)

"Should consumer data protection be given a low priority in light of the more pressing need for financial inclusion?

…

Here, it is important to remember how we began: financial inclusion is not an end in itself but a means to other ends, including permitting the poor and those living in remote areas to support their families, prosper, gain control over their financial destinies, and feel a sense of pride and belonging in their broader communities. The harms caused by unregulated data practices work against each of these goals."

DP4DFS, COVID-19 AND OTHER EMERGENCIES

COVID-19 and other global and national emergencies have highlighted the need to consider DP4DFS issues. The fundamental importance of DFS in preserving the functioning of the financial system, enhancing security and alleviating poverty during global emergencies such as COVID-19 has been well-recognized, including in the AFI Policy Framework for Leveraging Digital Financial Services to respond to Global Emergencies – Case of COVID-19 (2020). The reasons include the ability of DFS to facilitate the delivery of low-cost G2P cash transfers, emergency credit and, local and international remittances. DFS also enables accounts to be operated and payments for goods and services to be made in a remote, contactless way.

However, the explosion in the use of DFS during crisis such as COVID-19 raises data privacy challenges. The scale of existing data privacy concerns is likely to be exacerbated in an emergency. This is because the usual controls over identification information or the privacy of payments data may be waived or ignored in an emergency for the benefit of the private sector and/or government agencies.[13] This may happen because of the urgent need to identify individuals entitled to emergency assistance. Another consideration is the extreme demand for receipt of funds, which may make it even less likely that data subjects will read privacy disclosures or be able to provide effective consent. These concerns exist alongside other data privacy and protection issues (for example, relating to the increased risk of cyber fraud, the need to ensure the privacy of health information and of personal data loaded on COVID-19 related location apps).

9 OECD: Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-Centric Analysis (2020) (section 1.6)

10 CGAP: Focus Note - Is Data Privacy Good for Business? (2019) and CGAP: Blog - Data Privacy Concerns Influence Financial Behaviours in India, Kenya (2020)

11 Toronto Centre: Cloud Computing: Issues for Supervisors (2020)

12 BIS Basel Committee on Banking Supervision: Report on Open Banking and Application Programming Interfaces (2019) (Executive Summary and section 6)

13 IMF: Special Series on COVID-19 - Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies (2020)

EMERGING TRENDS IN DP4DFS POLICY AND REGULATORY

GENERAL DATA PRIVACY LAWS

There is an increasing trend to establish data privacy regulatory frameworks, which reflect the significance of the above-mentioned data processing developments.

The UNCTAD database on Data Protection and Privacy Legislation Worldwide indicates that 66 percent of countries have such legislation, with another 10 percent having draft legislation. The DLA Piper Data Protection Laws of the World also provides an overview of data privacy and protection laws in 116 jurisdictions.

The most well-known example of a general-purpose data protection regulatory framework is probably the EU's General Data Protection Regulation (GDPR),[14] **but there are other leading examples.** Many emerging, as well as developed, economies have enacted far-reaching data privacy and protection laws in recent years. Examples of AFI members with such laws include Ghana, Malaysia, Kenya, Mexico, Peru, the Philippines, and South Africa. India also has an advanced draft of such a law and Rwanda's Cabinet has also recently approved a draft law relating to data protection and privacy.[15] See Annex 2 for details. These laws are of general application in the sense that they apply to all forms of data processing for any purpose, i.e., not just financial services. However, they reflect a number of emerging trends relevant to DFS, the more significant of which are discussed below.

A RISK - BASED PROPORTIONATE APPROACH

It is generally accepted that a risk- based proportionate approach should be a key consideration in regulating innovative market developments, including those relevant to DP4DFS. This is the approach reflected in the proposed Guiding Principles. As noted in AFI's Special Report on Creating Enabling Ecosystems: The Role of Regulators (2020): 'to regulate innovative market deployments, many AFI member countries, such as Kenya, Tanzania and the Philippines, are implementing proportionate regulatory approaches'.[16] The concept of 'proportionality' is defined in AFI's Policy Model on Consumer Protection for Digital Financial Services (2020) as 'ensuring that regulatory responses reflect the business model, size, systemic significance, as well as the complexity and cross-border activity of the regulated entities'.[17]

A risk-based proportionate approach is especially important in the FinTech and financial inclusion context, given the desire not to dampen DFS innovation or competition. This may occur with over-burdensome regulatory requirements, especially for smaller FinTech entities with limited incentives and resources to manage privacy risks. Another important consideration is that regulators in developing countries may not have the resources or technical capacity to supervise complex DP4DFS standards. The challenge is to ensure a balance between these considerations and DP4DFS risks, coupled with the need to encourage financial inclusion and the trust of data subjects.

Regulators would need a data privacy risk assessment methodology for a risk-based DP4DFS approach. Any such methodology would need to have regard to the common risk factors in data processing by DFS business models, including those arising from information sources, information sensitivity, use cases and interconnectivity of systems. AFI is considering publishing a paper on this issue.

In order to address proportionality, consideration may be given to imposing obligations by reference to the significance of data processing activities. Relevant factors could include, for example:

- The nature of the DFS products or business model;
- The volume and sensitivity of data processed;
- The number of data subjects;
- Turnover of the data fiduciary;
- The risk of harm from the processing; and
- New technologies used.

14 https://gdpr.eu/

15 https://www.primature.gov.rw/index.php?id=131&tx_news_pi1%5Bnews%5D=933&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=7a012c144e6b2eb6d384a0bf1f153c26

16 https://www.afi-global.org/publications/3181/Creating-Enabling-FinTechFinTechFinTechFinTech-Ecosystems-The-Role-of-Regulators

17 https://www.afi-global.org/publications/3465/Policy-Model-on-Consumer-Protection-for-Digital-Financial-Services . This definition also appears in G20/OECD Policy Guidance: Financial Consumer Protection Approaches: Financial Consumer Protection in the Digital Age (2018)

The precise obligations imposed on a 'significant data controller' are likely to depend on the country context. For example, it may be that only "significant" data controllers are required to be registered; to prepare a data privacy impact assessment for specified processing activities; to appoint a data protection officer or to prepare annual compliance reports or have them audited. Examples are in Kenya's Data Protection Act 2019, as well as in India's draft Personal Data Protection Bill 2019.

Alternatively, obligations may be framed in terms of taking 'reasonable' steps, or some other moderating standard. The Philippines Data Protection Act (2019), for example, refers to 'reasonable' rights of access, 'reasonable' data correction requests from the data subject and 'reasonable and appropriate' security requirements.[18] Further guidance as to the meaning of 'reasonable' is helpful with this approach, such as through regulations and guidance issued by the DPA.

Another approach to proportionality is to exempt clearly defined "small businesses" from any obligation to comply with a data privacy regulatory framework. Australia currently provides a rare example of this approach, with its exemption for most 'small businesses' (those with an annual turnover of A$3 million or less).[19] However, the exemption is under review in Australia.[20] The difficulty with this approach is that it does not take into account the privacy impact on data subjects of the activities of the small business. A 'small" FinTech entity, for example, could have very few employees but use advanced and opaque data processing tools and techniques to process huge volumes of personal data, including sensitive data. Further, such an approach does not create a level playing field and raises the risk of regulatory arbitrage.[21]

For completion, where data privacy rights are recognized by local law, than any limitation on those rights should also be proportionate to the risks faced by the data subject. For example, the processing of personal data should only be permitted to the extent necessary for the purposes for which the data was collected and having regard to any consent provided. Further, any limitation on data privacy rights should be thoughtfully justified and proportionate safeguards required.[22]

BOX 5: PROPORTIONALITY REQUIREMENTS IN INDIA

The Supreme Court of India noted the following 4 'proportionality' requirements in considering the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act (2016) and limitations to India's constitutional right to privacy:

(a) A measure restricting a right must have a legitimate goal (legitimate goal stage).

(b) It must be a suitable means of furthering this goal (suitability or rationale connection stage).

(c) There must not be any less restrictive but equally effective alternative (necessity stage).

(d) The measure must not have a disproportionate impact on the right holder (balancing stage)

Source: Justice K.S. Puttaswamy vs. Union of India (Judgement of 26 September 2018

DP4DFS RISK MITIGANTS

The data privacy laws reviewed for the purposes of this Guideline Note contain mitigants to data privacy risks. Table 2 below summarizes the more common of these mitigants by reference to the privacy risks described above. The mitigants are likely to vary between countries, to be more detailed in practice and may be subject to qualifications and exceptions.

Following the table there is further explanation of the more important mitigants and related concepts, including a discussion of specific proportionality issues.

Clarity is also being provided as to the procedure for exercising data subject rights. This is an important issue given the complexities of the FinTech environment and the need for data subjects to be aware of how they may exercise their rights. For example, the regulations made under Mexico's Law on the Protection of Private Data held by Private Parties (2012) contains extensive provisions on the procedures for exercising rights of access, rectification, cancellation, and objection (ACRO) rights (Chapter VII).

18 Philippines: Data Protection Act (2019) (sections 16 and 20)

19 Office of the Australian Information Commissioner: Small Business (accessed 14 December, 2020) and related definitions in Australia: Privacy Act 1988 (Division 1 of Part 1)

20 Australia: Attorney – General's Department: Privacy Act Review Issues Paper (2020)

21 See G20 High-Level Principles for Digital Financial Inclusion (2016) (Principle 3)

22 European Data Protection Supervisor: The EDPS quick-guide to necessity and proportionality (2020).

TABLE 2: DP4DFS RISKS AND MITIGANTS

DATA PRIVACY RISKS	MITIGANTS – DATA CONTROLLER OBLIGATIONS	MITIGANTS – DATA SUBJECT RIGHTS
NO CONTROL OVER PROCESSING OF PERSONAL DATA	**Lawful processing:** Processing is required to be 'lawful', which usually means there is consent from the data subject or the processing is necessary for the purposes of a contract, a legal requirement, or in order to protect the vital interests of the data subject or those of the data controller. **Transparent information:** Information is to be provided to the data subject on collection of personal data covering issues such as: the purposes and sources of collection; the types of information to be collected; to whom it may be disclosed; contact details for the data controller; and the data subject's rights. Further, all information should be clearly and simply expressed and in a language that the data subject is likely to understand. **Requests for consent:** Consent requests are required to be presented separately from other information, to be specific and to be freely given and informed. **Fairness requirement:** Data processors are required to treat data subjects' fairly'. This concept is not normally defined and may require regulatory guidance. **Purpose limitation:** Personal data can only be processed for the primary/specific purpose of collection unless an exception applies (such as consent). This mitigant may be a variation of the 'lawfulness' mitigant. **Data minimization:** The data processed should be adequate and relevant and limited to the minimum necessary for the purposes of the processing.	**Right to information:** The data subject has the right to clear, simple information about processing activities and the entities involved. **Right to erasure/to be forgotten:** The data subject has the right to ask for their personal information to be erased after it is no longer necessary for the purpose for which it was processed. **Right to restrict processing:** The data subject may ask for processing to be restricted in certain circumstances, such as when accuracy is contested, or the processing is unlawful. **Right to portability:** The data subject can ask for personal data, which has been automatically processed to be provided to them in a structured, commonly used, machine readable form. **Right to withdraw consent:** The data subject may withdraw consent at any time.
SENSITIVE DATA MAY BE COMPROMISED	**Express consent**: Require that prior, express consent be obtained to the processing of "sensitive" information. See Annex 3 for a suggested definition of this concept.	
INCORRECT, MISLEADING, INCOMPLETE, OR OUT OF DATE PERSONAL DATA MAY BE PROCESSED	**Data quality:** The data controller is obliged to take at least reasonable steps to ensure data which is processed is accurate and up-to-date. **Time limit on retention:** Personal data can only be retained for the period necessary to satisfy the purpose of processing.	**Right to correction:** The data subject has the right to ask that their information be corrected. **Right to access:** A data subject is entitled to have access to their information on request and to details of any processing activities and who has undertaken them.
AUTOMATED DECISION MAKING, INCLUDING PROFILING MAY LEAD TO UNFAIR DECISIONS	**Information about automated processing:** Require that the data subject be given meaningful information about any automated decision-making process (including profiling) and its possible consequences, at the time the personal data is collected.	**Right to object:** A data subject has the right to object to the making of decisions based solely on automated processing of their personal data.

TABLE 2: *CONTINUED*

DATA PRIVACY RISKS	MITIGANTS – DATA CONTROLLER OBLIGATIONS	MITIGANTS – DATA SUBJECT RIGHTS
IDENTIFY FRAUD AND MISUSE OF OFFICIAL IDs MAY OCCUR	**Treat identity information as a category of 'sensitive information':** This information should require express consent for processing. Further mitigants are likely in laws establishing national ID systems and more generally in security requirements applicable to personal data processing systems and in criminal laws.	**Consumer awareness:** Require that data subjects be educated as to how to best secure their identity information, including their security credentials.
RECOURSE RIGHTS MAY BE LIMITED.	**Accountability:** Make the data controller responsible for their own actions and those of any processor who acts on their behalf. **Complaints systems:** Require data controllers to have a transparent, effective, free systems in place to process complaints about misuse of personal data. **Appeals:** ensure that there is in place an External Dispute Resolution (EDR) scheme to mediate on disputes between a data subject and a data controller and make appropriate orders (e.g., as to compensation or data correction). The EDR scheme is commonly provided by the relevant DPA. **Limits on cross border transfers of data:** Require that cross-border transfers of data only be made to jurisdictions that have equivalent privacy protections to those in the transferee jurisdiction, and/or that there are appropriate contractual safeguards. There may also be data localization rules in place. **Registration of data controllers:** There may also be requirements for data controllers to be registered by the relevant DPA. This obligation may only apply to the more significant data controllers.	**Awareness of complaints processing systems and EDR scheme:** Data subjects should be informed about their rights and relevant complaints and appeals avenues by the data controller when data is provided and on making a complaint.
DATA CONTROLLER SYSTEMS AND PROCEDURES DO NOT ENSURE DATA PRIVACY.	**Governance arrangements:** Require data controllers to have in place detailed policies and procedures designed to ensure compliance with the relevant data privacy principles and rules, together with related technological and organizational resources. **Privacy Impact Assessments (PIAs):** Require that high risk processing operations be the subject of proactive PIAs, which cover issues such as the proposed processing activities and the related privacy risks and mitigants. **Publicity:** Require privacy policies and PIAs to be made public (e.g., on the data processor's website). **Data Protection Officers:** Require that data controllers appoint a DPO with functions, such as overseeing compliance with any data privacy rules and being a contact point for data subjects and any DPA. This obligation may only apply to the more significant data controllers.	

Some of the above mitigants may be controversial. There are differing opinions as to the efficacy or appropriateness of some of the mitigants, as well as concerns as to whether there is an appropriate balance between the relevant risks and the mitigants.

Examples of these controversies include the apparent tension between data minimization rules and the era of big data and machine learning[23] and the debate as to whether the right to be forgotten is realistic given blockchain technology.[24]

AUTOMATED DECISION MAKING

There is an increased focus on the risks associated with automated decision marking, including bias against women/other vulnerable segments and profiling. In summary, the concern is that decisions about a data subject which are made on the basis of automated processing and profiling without any human intervention may result in discrimination and unfair biases.

A further concern is that data subjects are not likely to understand complex, constantly evolving algorithms used in such processes.[25] The box below provides some examples of different regulatory approaches to these risks.

BOX 6: AUTOMATED DECISION MAKING

The following are examples of rules concerning automated decision making, including profiling (in summary).

EU: General Data Protection Regulation (2016)
A data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects the data subject (Article 22). Exceptions apply where consent has been given or the decision is necessary for entering into a contract or its performance or the processing has been expressly authorized by law with appropriate safeguards.

'Profiling' means, in summary, automated processing, which uses personal data to evaluate personal aspects of a person (e.g., to analyze or predict work performance or health, economic performance, preferences, interests, reliability, location or movements) (Article 4).

Philippines: Personal Data Protection Act (2012)
A data subject has the right to information about automated processes where the data may be the sole basis for a decision affecting the data subject (section 16)

BOX 6: *CONTINUED*

Ghana: Data Protection Act (2012)
An individual may require a data controller to ensure that decisions significantly affecting the individual are not based solely on automated processing of data. The data controller then has 21 days to advise of the steps they will take to comply. However, there are exceptions to these requirements, including where the processing relates to a decision to enter into a contract (section 41).

CONSENT

There is an increasing emphasis on the need for fair and effective data processing consents. Many of the AFI knowledge products listed in Annex 5 refer to this issue. For example, the AFI Policy Model for E-Money 2019 advocates requiring e-money issuers to obtain informed consent for access to demographic or personal information (Part VI). Many laws also require consent from a data subject to the processing of their data unless an exception applies. Common exceptions are processing required or allowed by law or processing required to perform a contract. In broad terms, there is now an increased emphasis on the need for:

- Freely given, informed and unambiguous consents;
- Consent to be given for a specific purpose;
- Requests for consent being separated from other information;
- Consent being able to be withdrawn; and
- The data controller or processor to have the burden of proving consent was given.

See the examples in Box 7 on the next page.

However, there is an ongoing debate as to whether the consent model is 'broken'. The concerns have arisen because consent is the foundation behind many data privacy frameworks and there are fundamental concerns as to whether data subjects can give free and informed consent.

23 ITU: Financial Inclusion Global Initiative (FIGI) Security Infrastructure and Trust Working Group, Big data, machine learning, consumer protection and privacy (2018)

24 Finextra: Blog by Carlo R.W. de Meijer Economist and Researcher at De Meijer Independent Financial Services Advisory (MIFSA): Blockchain versus GDPR and who should adjust most (2018)

25 CFI Blog: Data for Inclusive Finance: Delivering on the Promise for Consumers (2020)

BOX 7: EXAMPLES OF STRENGTHENED CONSENT REQUIREMENTS

EU: General Data Protection Regulation (2016)
Processing of personal data is only lawful to the extent that the data subject has given their specific consent to the specific purpose of the processing or another exception applies (Article 6).

The concept of 'consent' is defined as: 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Article 4(11)).

Other GDPR rules in Article 7 require that the consent request be:

- 'clearly distinguishable' from other matters;
- In an intelligible and easily accessible form; and
- In clear and plain language.

The data subject must also have a right to withdraw consent at any time and it must be as easy to withdraw consent as it is to give it.

Malaysia: Personal Data Protection Act and the Personal Data Protection Code for the Banking and Financial Sector (BFS Code)
The Act states as a General Principle that data subjects must give their consent to the processing of personal data (with some exceptions) (section 6). Although the concept of 'consent' is not defined in the Act, the mandatory BFS Code provides examples of forms of consent for the commencement of a contract (including deemed consent, as well as signatures or ticks indicating consent, opt-in consent and verbal consent). There is also provision for consents to be provided for by electronic channels including SMS, e-mail, and messaging systems). In all cases, the form of consent must be recorded and maintained.

Peru: Personal Data Protection Law (2011) and Regulation for Law (2013)
One of the Guiding Principles under the Law is that the data subject must give their consent to processing of their personal data (with specified exceptions). The consent must be 'prior, informed, express and unequivocal' and may be revoked at any time (Articles 5 and 13). Peru's Personal Data Protection Regulation contains detailed rules and examples as to the meaning of this concept of consent and makes it clear that it may be given electronically.

Philippines: Data Privacy Act 2012 and Implementing Rules and Regulations
Consent is required to the collection and processing of personal information (subject to exceptions) (section 12). The concept of 'consent of the data subject' is

BOX 7: *CONTINUED*

defined as '… any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means....' (section 3(b)). The Implementing Rules and Regulations also provide for consents to be time-bound and to be able to be withdrawn (section 19)

South Africa: Protection of Personal Information Act 2013
Processing of personal information requires consent (unless an exception applies) (section 11). The responsible party has the burden of proving consent. The concept of consent is defined to mean 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information' (section 1). Further, there is a requirement that consents for direct marketing by electronic communication be in a prescribed form (section 69, regulation 6 and Form 4).

This is especially the case in a financial inclusion context, where data subjects are likely to have low levels of financial capability.[26] Key concerns include:

- Long, complex forms of consent;
- Consents that are 'buried' in lengthy terms and conditions;
- Lack of choice – the data subject may feel they have to consent if they want the DFS;
- Bundled consents, which cover data processing for the DFS and e.g., direct marketing;
- Inability to withdraw a consent;
- Consents being addressed to multiple entities e.g., the DFS provider and service providers;
- Not being able to retain forms of consent for future reference; and
- Consents being in a language the data subject does not understand.[27]

26 World Bank: Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting (2018)

27 McDonald AM and Cranor LF The Cost of Reading Privacy Policies A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568 (2008). This study found that it would take the average person 244 hours a year to read online privacy policies!

Consideration is now being given to alternatives to consent. For example, CGAP has advocated both a legitimate purposes approach and a data fiduciary approach as alternatives to the consent model in their recent publication CGAP Making Data Work for the Poor (2020). The need for consent is not however, likely to disappear entirely given the likelihood that consent will always be required in some cases – for example, express consent to process sensitive information and express consent for direct marketing or cross selling purposes. Further, consent is the foundation of new approaches to open banking systems.

There are approaches, which may go some way to alleviating the abovementioned defects with the consent model. Examples include:

- Mandating an overriding general principle to process data fairly (or similar concept)[28];
- Treating financial data as a special category of data which requires express consent for processing[29];
- Supporting the statutory consent requirements described above with detailed rules as to what is needed for each element of the consent requirement (for example as to the meaning of "freely given", "prior", "express" and "informed" and how forms of consent may be presented, and given, in a digital environment);[30] and
- The use of third parties to manage the consent process in open banking systems (see Box 8).

DIGITAL IDS AND RISKS OF IDENTITY FRAUD, MISUSE, AND INAPPROPRIATE ACCESS

There is global recognition of the advantages of digital ID systems for development goals. As noted in World Bank: Digital ID and the Data Protection Challenge: Practitioner's Note (2019), they can include (in summary):

- Facilitating access to 'rights, services, and economic opportunities that require proof of identity' (such as DFS services including credit, payments, savings, insurance, and pensions);
- Strengthening of governance and service delivery (for example, by minimizing public sector fraud in G2P payments whilst facilitating G2P cash transfers);
- Supporting the private sector in complying with identity requirements such as eKYC rules; and
- Enabling the digital economy (for example, through facilitating trusted transactions and creating innovation opportunities).

BOX 8: CGAP: INDIA'S NEW APPROACH TO PERSONAL DATA-SHARING (2020)

Consent and India's Account Aggregator Model

"Data-sharing among financial services providers (FSPs) can enable providers to more efficiently offer a wider range of financial products better tailored to the needs of customers, including low-income customers. However, it is important to ensure customers understand and consent to how their data are being used.

India's solution to this challenge is account aggregators (AAs). The Reserve Bank of India (RBI) created AAs in 2018 to simplify the consent process for customers. In most open banking regimes, financial information providers (FIPs) and financial information users (FIUs) directly exchange data. This direct model of data exchange—such as between a bank and a credit bureau—offers customers limited control and visibility into what data are being shared and to what end. AAs have been designed to sit between FIPs and FIUs to facilitate data exchange more transparently. Despite their name, AAs are barred from seeing, storing, analyzing, or using customer data. As trusted, impartial intermediaries, they simply manage consent and serve as the pipes through which data flow among FSPs. When a customer gives consent to a provider via the AA, the AA fetches the relevant information from the customer's financial accounts and sends it via secure channels to the requesting institution."

- See also: Reserve Bank of India: Master Direction-Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions (2016)

Conversely, there is recognition of the privacy-related risks associated with digital IDs. The scale of these risks has potential to be enormous, given the sheer size of the data sets and the centralization of data.[31] These risks may be summarized as follows:

- Identity fraud is a particular concern with digital IDs, which rely on biometrics as they are not secret and compromised biometric identity data cannot be corrected;

28 Philippines: Personal Data Protection Act (2012) (section 11(2)) and Rule IV section 19(b) of Implementing Rules and Regulations

29 Mexico: Federal Law on Protection of Personal Data held by Private Parties (2010) (Articles 8,10 and 37) and Regulations (Article 15)

30 See, for example, Peru: Personal Data Protection Law (2011) and Regulation for Law (2013) (see especially Article 7 of Regulation and Chapter I and II of Title III).

31 World Bank: Digital ID and the Data Protection Challenge: Practitioner's Note (2019)

- Identification without consent – this might be done through:
  - Unauthorized use of biometric data such as fingerprints or iris scans or facial recognition information;
  - Identifying a person across multiple domains of service through the use of their digital ID;
- Illegal surveillance of individuals through following use of digital IDs;
- Inappropriate requests for a customer to identify themselves by providing their digital ID, with consequential risks of commercial exploitation; and
- Misuse of digital ID information in the public domain through inappropriate use and sharing across government agencies.[32]

The above risks are especially relevant to DFS. They can mean, for example, that an individual's identity is misused to obtain credit, government subsidies or cash transfers; to open a savings account, which is used for illegal activities; or to obtain access to funds in online investment or retirement accounts. These risks have led to demands for privacy protection frameworks.

For further discussion of the benefits and risks of digital ID systems see: the AFI Special Report on FinTech for Financial Inclusion: A Framework for Digital Financial Transformation (2018) (Pillar 1) and also AFI: KYC Innovations, Financial Inclusion and Integrity In Selected AFI Member Countries (2019).

PRIVACY BY DESIGN

Proactive privacy by design rules is another important innovation, which can minimize DP4DFS risks to data subjects. The principles behind these rules are well known,[33] but they have only just started being introduced into data privacy frameworks. In summary, the idea is that DFS providers should have documented governance arrangements, policies, procedures, and resources to ensure that they comply with data privacy rules at all times. Further, the default setting of systems should ensure compliance (for example, with the rule that only the minimum data needed for the permitted purpose of collection is processed). In practice, compliance with such requirements by DFS providers might be reviewed by regulators in considering license or registration applications, requests for approval of new DFS products or in a regulatory sandbox context.

One example is in Kenya's new Data Protection Act (2019) under section 41 'Data protection by design or by default'. These requirements, which are similar to those in Article 25 of the GDPR, require (in summary) data controllers and processors to put in place appropriate technical and organizational measures:

- To implement Kenya's data protection principles and necessary safeguards; and
- To ensure that, by default, only personal data necessary for each specific purpose is processed, taking into account specified factors such as the amount of personal data collected, the extent of processing, the storage period and processing costs.

Kenya's Data Protection Act also contains requirements for data controllers and processors to consider relevant risks to personal data, safeguards, the pseudonymization and encryption of personal data and also the ability to restore data.

Another example of requirements for privacy by design is in India's draft Personal Data Protection Bill (2019). The Bill requires every data fiduciary to prepare a detailed privacy by design policy. The policy may be submitted to the DPA for certification and any certified policy must be published on the website of the data fiduciary and of the Authority (section 22). The publication of the policy is an important requirement as it is likely to improve transparency for data subjects and investors, as well as the DPA and other regulators and government agencies.

DATA PRIVACY IMPACT ASSESSMENTS

Some countries also have requirements to assess the privacy impact of a particular data processing operation. These requirements may be additional to Privacy by Design requirements. For example, Kenya's Data Protection Act (2019) requires that a 'data protection impact assessment' must be prepared in relation to a processing operation if it is likely to result in 'high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purposes'.[34] In summary, it requires a systematic description of the proposed processing requirements and their necessity and proportionality and of the risks to the rights and freedoms of data subjects and the measures to be taken to alleviate them.

32 For a discussion of these issues see the decision of the Supreme Court of India in Justice K.S. Puttaswamy vs. Union of India (2017) 10 SCC 1 which struck down legislative provisions allowing corporates and individuals to seek identification via India's Aadhaar identifier – see https://www.scobserver.in/court-case/constitutionality-of-aadhaar-act/plain-englishsummary-of-judgment

33 Cavoukian, Ann 'Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices' (2011)

34 Kenya Data Protection Act (2019) (section 31).

There is also provision for the Data Protection Commissioner to be consulted and for the Data Protection Commissioner to publish guidelines.[35] Australia's Office of the Australian Information Commissioner has issued a Guide to Undertaking Privacy Impact Assessments and related advice on assessing privacy risks and an e-learning course.[36] India's draft Personal Data Protection Bill (2019) is also quite specific in requiring a significant data fiduciary to conduct a data protection impact assessment in these cases: where the processing involves new technologies or large scale processing or the use of sensitive data (such as genetic or biometric data) or if the processing carries a risk of 'significant harm'.[37]

REGISTRATION OF DATA CONTROLLERS AND PROVIDERS

Some developing countries are now requiring data controllers to be registered. Ghana's Data Protection Act (2012), as noted above, requires registration of all data controllers.[38] Kenya's Data Protection Act (2019) is to the effect that the Data Commissioner may prescribe thresholds for mandatory registration of data controllers and data processors.[39] Considerations relevant to requiring registration include:

- Whether registration will assist in achieving data privacy objectives, and to what extent;
- Whether requiring registration is a proportionate response to data privacy risks; and
- Supervisory capacity and resources to oversee the registration process.

DATA PRIVACY OFFICERS

Provision is increasingly being made for the appointment of data privacy (or protection) officers (DPOs). For example, the data privacy regulatory regimes in Ghana, Kenya, Mexico and Brazil have such provisions. The appointment seems to be optional in some cases. In other cases, it depends on factors such as whether the nature, scope, context, and purposes of the processor's activities are sufficiently large and/or significant and on the type of data that is processed. For example, the processing of sensitive data may suggest a DPO should be appointed.

The functions of DPOs vary but, in general terms, may include:

- Advice on compliance with the regulatory framework;
- Being a contact point for data subjects with queries or complaints;
- Being a contact point with the relevant DPA and other regulators and agencies;
- Consulting on Privacy Impact Assessments; and
- Facilitating capacity building of staff and agents.

REPORTING DATA PRIVACY BREACHES

Requirements to report unauthorized access to personal data are being introduced. For example, Kenya's Data Protection Act (2019) provides, with some exceptions, that where there has been unauthorized access to personal data and 'there is a real risk of harm' to the data subject then the Data Commissioner must be notified within 72 hours. The data subject must be notified in writing within 'a reasonably practicable period' and provided with sufficient information to take protective measures.[40] Other countries with requirements to notify either the DPA and/or relevant data subjects include Ghana, Mexico, Peru and Australia.

OPEN BANKING

Open banking regimes are being introduced in various countries and regions, including developing and emerging economies, raising important data privacy issues.[41] In summary, the concept of 'open banking' generally refers to systems for the sharing of customer data by financial institutions with third parties (such as other financial institutions, payments service providers, data aggregators, and commercial partners). The data privacy issues of concern include the need for express consent and the need to ensure that data subjects understand what they are agreeing to. There are of course also data protection issues (such as security issues), which are beyond the scope of this Guideline Note. Examples of such schemes in different forms are to be found in the data sharing rules in Mexico's Financial Technology Institutions Law (2018);[42] in the provisions concerning the ability of payments systems and service providers to access, process and retain personal data in the EU's EU Directive 2015/2366 on

35 Kenya's new Data Protection Commissioner (Ms. Immaculate Kassait) was sworn in on 6 November 2020. See https://www.capitalfm.co.ke/news/2020/11/immaculate-kassait-sworn-in-as-inaugural-data-commissioner/

36 https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

37 India Personal Data Protection Bill (2019) (section 27 and see definition of 'significant harm' in section 3

38 Section 27

39 Section 18

40 Section 43

41 BIS Basel Committee on Banking Supervision: Report on Open Banking and Application Programming Interfaces (2019)

42 Article 76

Payments Services (PSD2);[43] and in Australia's open banking rules and the related Customer Data Right.[44]

CONSUMER RECOURSE

Provision is being made for complaints to be made by data users about breaches of their data rights. For example, as noted above, regulations made under Mexico's Law on the Protection of Private Data held by Private Parties (2012) contain extensive provisions on the procedures for exercising ACRO rights. Another example is provided by Chapter III of Title IV 'Protection Procedure' in the regulation made for the purposes of the Philippine's Data Privacy Act (2012).

It is common to allow complaints to be made to the relevant DPA. These rights can usually only be exercised if the complaint has first been submitted to the data controller or processor and they have either given an adverse decision or failed to deal with the complaint in a reasonable time period. For example, under South Africa's Protection of Personal Information Act (2013) complaints can be made to the Information Regulator. Further, compensation may be awarded on the basis of a civil claim instituted by the data subject or by the Information Regulator at the request of the data subject. There is also provision for codes of conduct issued by the Regulator to include provisions for dealing with complaints, which must meet the prescribed standards and any guidelines issued by the Regulator. Other countries also provide for some or all of these issues. Examples are in the data protection laws of Ghana, Malaysia, Mexico, and the Philippines.

Provisions allowing the DPA to initiate actions on behalf of data subjects are rare. South Africa is one example. Australia's OIAC may also investigate an interference with privacy on its own initiative and make a determination for compensation or require other remedial action. It is important that DPAs should have such powers in a financial inclusion context, given the likelihood that data subjects may not have the resources or capacity to bring such actions, or clear awareness as to their rights.

DATA PRIVACY IN EMERGENCIES

Some countries provide relief from the strict rules in data privacy frameworks to allow for data flows to assist in responses to emergencies (such as COVD-19). A rare example comes from Australia. In summary, Part VIA of Australia's Privacy Act (1988) provides for the making of emergency declarations that allow the collection, use and disclosure of information for a permitted purpose. These purposes relevantly include assisting individuals in obtaining financial or other humanitarian assistance. The declarations can apply for a limited time period up to 12 months. Where an entity validly relies on such a declaration then they will not be liable for breaching specified laws or codes, including the Australian Privacy Principles or a registered code.

Guidance on data privacy issues in the context of COVID-19 has also been provided by international agencies. The AFI Policy Framework for Leveraging Digital Financial Services to respond to Global Emergencies – Case of COVID-19 (2020), for example, suggests that "DFS providers should ensure consumer data is protected and not shared with third parties. Under extraordinary circumstances if customer data must be extracted (for contact tracing and containment of transmission), it must be done in a voluntary manner. Further, such measures should be temporary in nature.' (Pillar III Enabling Regulations).

The OECD has also made a number of recommendations on data privacy in their guidance on COVID-19. The headline key recommendations are (in summary):

- Governments need to promote the responsible use of personal data;
- Governments should consult Privacy Enforcement Authorities (PEAs) before introducing measures that risk infringing on established privacy and data protection principles;
- PEAs should address regulatory uncertainties;
- Subject to necessary and proportionate safeguards, governments should support national and international co-operation in collecting, processing, and sharing personal health data; and
- Governments and data controllers should be transparent and accountable.[45]

BOX 9: OECD: ENSURING DATA PRIVACY AS WE BATTLE COVID-19 (2020)

'Policy makers, in consultation with privacy enforcement authorities, must assess the possible trade-offs in data utilization during this crisis (reconciling the risks and benefits), but must ensure that any extraordinary measures are proportionate to the risks and are implemented with full transparency, accountability and a commitment to immediately cease or reverse exceptional uses of data when the crisis is over.'

43 Article 94
44 See https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0
45 OECD Ensuring Data Privacy as we Battle COVID-19 (2020)

GSMA has also released COVID-19 Privacy Guidelines for mobile network operators.[46] They may be relevant to mobile phone-based DFSs and related privacy issues. The focus is on disclosures to governments and agencies. The Guidelines cover issues such as the need to comply with ethical considerations as well as the law; transparency about disclosures; and disclosures of metadata and aggregated non-identifiable data.

PENALTIES

Significant penalties are now also being imposed in newer data privacy regulatory frameworks. Large scale penalties may provide an incentive for compliance, as well as an incentive to invest in Privacy Enhancing Technologies (PETS) (which are beyond the scope of this Guideline Note).

There are a variety of approaches as to how penalties may be determined. In some cases, they are based on a percentage of annual turnover. For example, the EU's GDPR provides for a maximum penalty of up to four percent of the global annual turnover of the entity. Kenya's new Data Protection Act (2019) takes a less strict approach in providing for the maximum penalty to be the lower of a maximum penalty of five million shillings (approx. USD 45,700)[48] or one percent of the annual turnover of the preceding financial year. Other countries such as Malaysia make provision for a fine of a maximum amount and/or a term of imprisonment. Mexico's Federal Law on the Protection of Personal Data held by Private Parties takes an interesting approach in that potential fines are a multiple of the Mexico City minimum wage, with the amount varying depending on the breach. A final example comes from Peru, where violations are classified as mild, serious, or very serious with the level of fine varying accordingly.

REGULATORY SANDBOXES

It does not appear to be common for regulatory sandboxes established by financial sector regulators to specifically consider DP4DFS innovations. A regulatory sandbox, in brief, is an increasingly popular mechanism for the testing of FinTech innovations in a supervised environment. However, it does not appear to be common to test innovations related to data privacy in sandboxes, or in similar innovation forums established by financial sector regulators. Instead, countries such as Australia make it clear that entities relaying on regulatory sandbox exemptions must still comply with data privacy laws.[49]

However, there are a few examples of the sandbox concept being used in circumstances relevant to DP4DFS.[50] For example:

- The UK's Information Commissioner's Office (ICO) has established a sandbox, and their 2020-2021 key areas of focus include innovations related to data sharing, including in the area of finance.[51] Importantly, the ICO and the UK's Financial Conduct Authority also have a 2019 Memorandum of Understanding establishing a framework for cooperation, coordination and information sharing between the regulators.[52]
- There are also thematic sandboxes covering specific data privacy policy objectives. Examples of existing thematic regulatory sandboxes, including some relevant to financial inclusion and 'NextGen' technologies, are highlighted in the CGAP: Blog - A Growing Trend in Financial Regulation: Thematic Sandboxes (2019).

Regulatory sandboxes for data privacy innovations may also be provided for by legislation. A rare example is in India's draft Personal Data Protection Bill (2019) requires the DPA to create a 'Sandbox'. This is to be 'for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest" (section 40). Data fiduciaries who have had their privacy by design policies certified by the DPA are eligible to apply for inclusion in the Sandbox (subject to regulations which are yet to be developed).

SECTOR-SPECIFIC RULES AND GUIDANCE ON DP4DFS

As well as the above laws of general application, there are limited examples of regulatory frameworks, codes of practice, national strategies and policy interventions, which apply specifically to aspects of DP4DFS. Examples are provided below.

BOX 10: AFI POLICY FRAMEWORK FOR RESPONSIBLE DIGITAL CREDIT (2020)

'Consumer data protection is crucial in ensuring that digital credit, as well as other financial services, give consumers confidence that their data is private and being used appropriately.' (Principle 6: Data Protection and Privacy)

46 GSMA COVID-19 Privacy Guidelines (2020)

47 For a discussion of PETS and related issues see ITU: Financial Inclusion Global Initiative (FIGI) Security Infrastructure and Trust Working Group, Big data, machine learning, consumer protection and privacy (2018)

48 As at 15 November 2020 https://www.xe.com/

49 ASIC: INFO 248 Enhanced regulatory sandbox (2020)

50 Centre for Information Policy Leadership: Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice (2019)

51 https://ico.org.uk/sandbox

52 https://ico.org.uk/media/about-the-ico/documents/2614342/financial-conduct-authority-ico-mou.pdf

FINANCIAL SECTOR RULES FOR DP4DFS

Sector-specific rules may also be issued covering DP4DFS issues of special concern. A recent example comes from the Philippines (see Box 11).

BOX 11: PHILIPPINES NATIONAL PRIVACY COMMISSION CIRCULAR NO. 20-10 GUIDELINES ON THE PROCESSING OF PERSONAL DATA FOR LOAN RELATED TRANSACTIONS (2020)

The Philippines National Privacy Commission recently issued the above Circular following thousands of complaints about the use of mobile phone and social media data by online lenders, including for debt collection purposes. It applies to lending and financing companies and contains rules prohibiting the use of contact details for debt collection purposes, restricting the use of photos and other rules limiting the collection, use, disclosure, and retention of personal information. The NPC has separately ordered the cessation of processing activities by various online lenders[53] and the Securities and Exchange Commission has also taken action to revoke the authorization to operate of some such lenders.[54]

Banking, payments, and e-money regulatory frameworks may also contain data privacy rules. Examples include:

- The banker–customer duty of confidentiality/secrecy;[55]
- Rules on the privacy and protection of customer's personal information in financial consumer protection rules;[56]
- An obligation on applicants for e-money licenses to comply with applicable standards concerning data security and confidentiality;[57]
- Obligations to ensure confidentiality of customer information relating to payments instruments, including information in the possession of agents;[58]
- The ability of payments systems and payment service providers to access, process and retain personal data, (in the case of the EU's PSD2 this requires explicit consent, subject to exceptions such as fraud detection[59]); and
- The right of payment users to make use of account information services (PSD2 also requires explicit consent in this case, as well as compliance with other conditions).[60]

INDUSTRY CODES

Data privacy codes may be developed for financial services, including DFS. In general DP regulatory frameworks, it is common to make provision for sector-specific codes to be made by industry groups and/or the data protection regulator. Examples are in the DP frameworks for the EU, Australia, Brazil, Ghana, Kenya, Malaysia, Mexico, and the Philippines and South Africa. However, bearing in mind that such the relevant DP laws are likely to be quite new, examples of codes specific to financial services are rare. Malaysia provides one such example (see Box 12).

General purpose financial sector industry codes of practice may also contain privacy provisions. For example, the Philippines Banking Code for Consumer Protection, which was developed by the various banking associations, deals with privacy issues concerning disclosures to unrelated third parties for marketing purposes and telemarketing activities via email, telephone calls and text messaging (section 2(e)). Another example is South Africa's industry Code of Banking Practice, which contains provisions dealing with the privacy and confidentiality of personal information (section 6.1).

BOX 12: MALAYSIA: THE PERSONAL DATA PROTECTION CODE OF PRACTICE FOR THE BANKING AND FINANCIAL SECTOR (2017)

Malaysia's Personal Data Protection Act makes provision for the registration of 'data user forums' that may then prepare a mandatory code of practice on their own initiative or at the request of the Personal Data Protection Commissioner (Part II, Division 3). The code will be registered if the Commissioner is satisfied that it is consistent with the Act and due consideration has been given to the purposes of processing data by relevant data users, views of data subjects and the relevant regulatory authority (such as Bank Negara Malaysia (BNM)), and the code overall offers an adequate level of protection. The penalty for a breach of the Code is a fine not exceeding 100,000 ringgit (approx. US$2,425[61]) and/or imprisonment up to 1 year.

53 https://www.privacy.gov.ph/2019/10/npc-shuts-down-26-online-lending-companies/

54 For example, https://www.sec.gov.ph/pr-2020/sec-revokes-fcash-global-lendings-license/

55 For example: Afghanistan: Banking Law (1974) and Philippines: Secrecy of Bank Deposits Act (1955)

56 For example: Philippines: BSP Circular 857 – Regulation on Financial Consumer Protection (Chapter II, section (b) Protection of Client Information)

57 For example: Bank Indonesia Electronic Money Regulation (2018)

8 For example: India: Reserve Bank of India – Master Direction on Issuance and Operation of Prepaid Payment Instruments (2017) and Ghana: Payments Systems and Services Act (2019)

59 Article 94

60 Article 67

61 As of 15 November 2020 - https://www.xe.com/currencyconverter/convert/?Amount=10%2C000&From=MYR&To=USD

BOX 12: *CONTINUED*

The Personal Data Protection Code of Practice for the Banking and Financial Sector (2017) (BFS Code) is registered under the above provisions. The Code applies to all licensed banks and financial institutions and was developed by the Association of Banks in Malaysia. The Code summarizes relevant provisions of the Act, the related regulations and BNM's Product Transparency and Disclosure Guidelines and provides sector-specific examples of how they can be interpreted in practice. Emphasis is placed on explaining the definitions of personal, sensitive, and pre-existing data and rules concerning direct marketing and cross-selling, contacting the data subject and the transfer abroad of data. Templates are also provided for a Privacy Notice, a Data Access Request Form, and a Data Correction Request Form.

NATIONAL AND INTERNATIONAL POLICY GUIDANCE

National DPAs provide policy guidance relevant to DP4DFS. For example, the websites of the Philippines National Privacy Commission[62] and Ghana's Data Protection Commission[63] provide guidance on rights and responsibilities under the relevant laws, breach reporting, how to make a complaint and updates on the exercise of their powers.

Ghana provides a rare example of a national policy framework specifically for DFS. Box 13 describes the sections relevant to DP4DFS.

International agencies also provide guidance on regulatory and policy issues relevant to DP4DFS. For example, the World Bank Good Practices for Financial Consumer Protection (2017) provides guidance on the data protection and privacy issues applicable to retail payments. They were developed having regard to the 'Big Data" environment and other FinTech-related developments. (see Annex A, section D). In summary, it is suggested that there should be regulatory frameworks applicable to payment services providers (PSPs), which:

- Allow PSPs to collect customers' data within limits established by law or consent;
- Establish rules for the collection and retention of personal data;
- Limit use of personal data to purposes specified at the time of collection, permitted by law, or specifically agreed to by the customer;
- Require PSPs to maintain the confidentiality and security of personal data;

BOX 13: GOVERNMENT OF GHANA MINISTRY OF FINANCE DIGITAL FINANCIAL SERVICES POLICY (2020)

In May 2020 Ghana launched a four-year (2020 -2023) DFS Policy, reported by CGAP to be the first in the world. It is designed to serve as a blueprint for how Ghana can leverage digital finance to achieve its financial inclusion goals, complementing Ghana's National Financial Inclusion and Development Strategy. Data privacy and data security were noted as 'particularly important' in the DFS context, along with the comment: 'There are clearly DFS-specific risks that will need to be addressed by data protection framework.' Specific proposals on this point were (in summary):

- The Data Protection Commission (DPC) requires additional resources to complete the data controller registration process under Ghana's Data Protection Act (2012).
- DPC's technical capacity should be increased with training on data specificities in the DFS ecosystem.
- Cooperation between the DPC, financial sector regulators and the National Communications Authority should be facilitated through an MOU.
- The use of alternative data in the financial sector should be evaluated to determine if additional regulations are required.

- Make PSPs legally liable for misuse of personal data and any data security breaches;
- Prohibit PSPs sharing data with a third party for any purpose (including telemarketing or direct marketing) without prior written consent unless the third party is acting on behalf of the PSP and the information is used for purposes consistent with the original purpose of collection (unless an exception applies, such as a requirement under law);
- Allow consumers to opt out of sharing data previously permitted to be shared; and
- Develop specific rules for the third parties such as government authorities, credit registries and collection agencies.

Other international organizations have also developed guidance on good practices relevant to DP4DFS. Examples are in Annex 4.

62 https://www.privacy.gov.ph/
63 https://www.dataprotection.org.gh/

GUIDING PRINCIPLES FOR AN OVERALL DP4DFS FRAMEWORK INTRODUCTION

The Guiding Principles are intended as non-binding guidance for a framework for an overall risk-based, proportionate DP4DFS regulatory framework.

The framework has been developed on the assumption that there is not a general data protection law in place. The Principles reflect high-level emerging trends in data privacy rights and responsibilities. However, they should not be considered as best practice. In particular, depending on the country context, regulatory provisions may need to be more or less detailed than those proposed and to be subject to qualifications and exceptions. Finally, although the Guiding Principles have been framed having specific regard to data processing in the DFS context, they may be more generally relevant, including in relation to traditional financial services.

There are a number of ways that Guiding Principles could be implemented. They include:

- A new law;
- Regulations made, or guidance provided, for the purposes of an existing financial sector law; or
- A mandatory code of practice to be developed by industry associations and/or relevant regulators.

The extent to which the Guiding Principles are relevant for a country will depend on various factors. They may include the identified data privacy risks, the existing legal and regulatory framework, policy priorities, the mandate, and powers of regulators, supervisory capacity, and resources and whether there are industry associations which can effectively support the development, implementation, and enforcement of a code of practice.

There should be consultation on the preferred option with public and private sector stakeholders, and the public generally. This could include consultation
with Ministries and regulators covering the financial sector, telecommunications, competition, consumer protection and innovation generally. There should also be consultation with the private sector (including both traditional and FinTech DFS providers) and civil society stakeholders (such as consumer groups).

Consideration could also be given to regional data privacy initiatives. As noted in AFI Policy Framework for Responsible Digital Credit (2020) 'Where practical, regional cross-border initiatives can build confidence between countries, facilitate the sharing of best practices between policymakers and allow data privacy regulators to detect and address non-compliance more easily' (Principle 6).

A proposal has been included at the end of the Guidelines for a DP4DFS 'minimalist' risk-based and proportionate regime to be supervised by the lead financial sector regulator (such as the Central Bank). This proposal contains suggested interim priorities on the assumption that the supervisory capacity and resources which can be applied to DP4DFS are limited and also assuming that there is not a general data protection law in place.

THE GUIDING PRINCIPLES SET OUT BELOW ARE ORGANIZED INTO SIX PILLARS.

They include Key Recommendations for each Pillar. Where relevant, the Key Recommendations are organized on the basis that those that are considered easiest to implement should come first.

PILLAR 1:
DP4DFS POLICY AND REGULATORY FRAMEWORK

PILLAR 2:
DATA CONTROLLER AND PROCESSOR OBLIGATIONS

PILLAR 3:
DATA SUBJECT RIGHTS

PILLAR 4:
CONSUMER AWARENESS AND RECOURSE

PILLAR 5:
SUPERVISION AND ENFORCEMENT

PILLAR 6:
DP4DFS IN GLOBAL AND NATIONAL EMERGENCIES

PILLAR 1: DP4DFS POLICY AND REGULATORY FRAMEWORK

This Pillar is intended to cover the process for establishing the DP4DFS policy and regulatory framework and the related principles.

1.1. GUIDING PRINCIPLE: ESTABLISH GOVERNANCE AND CONSULTATION ARRANGEMENTS

KEY RECOMMENDATIONS:

- Establish Steering Committee with lead DP4DFS regulator and representatives of other financial sector regulators and other relevant government Ministries and agencies (e.g., for finance/ telecommunications / competition/ consumer protection/ innovation), as well as representatives of industry (including traditional financial sector and FinTech entities) and consumers (e.g., consumer associations).
- Ensure Steering Committee representatives have, or have access to, expertise covering DFS, data privacy issues and FinTech innovations in data processing for DFS.
- Engage outside experts as needed, e.g., data scientists or data privacy experts.
- Consult widely on new framework with public/ private sector stakeholders and general public.

1.2. GUIDING PRINCIPLE: ASSESS CURRENT DFS LEGAL AND REGULATORY FRAMEWORK AND MARKET

KEY RECOMMENDATIONS:

- Undertake a diagnostic analysis of existing legal and regulatory framework applicable to DP4DFS, including:
  - general data privacy and consumer protection laws
  - financial consumer protection laws
  - sector specific provisions in, e.g., e-money and payments laws
  - industry codes of practice
  - national strategies (e.g., for DFS or financial sector development or financial inclusion)
  - policy and regulatory guidelines
- Assess gaps/overlaps in regulatory framework and related supervisory mandate and powers by reference to Guiding Principles.
- Consider DFS market and related data privacy risks, including types of providers, controllers, and processors of personal data, DFS products, forms of consent, privacy policies, types of data and data analytics techniques used and any FinTech-specific issues.
- Consider needs of vulnerable groups, e.g., women, youth, the elderly, persons with disabilities and displaced persons.
- Assess any systemic complaints issues relating to DP4DFS.
- Document key benefits and risks of current environment for key stakeholders (especially data subjects and data controllers and processors).

1.3. GUIDING PRINCIPLE: ESTABLISH OVERARCHING POLICY AND REGULATORY PRINCIPLES

KEY RECOMMENDATIONS:

- Clarify regulatory principles to guide design of DP4DFS framework.
- Consider especially risk-based and proportionate rules, which provide a balance between privacy, data protection, innovation and competition and are:
  - clear and accessible
  - principles based
  - technology neutral
  - outcomes focused
- Require new framework to be activity-based so as to create a level playing field and minimize the risk of regulatory arbitrage (subject to following points).
- Consider whether some obligations should only apply to ‘significant’ data controllers such as obligations concerning:
  - Registration
  - Appointing a Data Privacy Officer
  - Preparing a Privacy Impact Assessment for high - risk processing operations
  - Breach reporting to regulators and to data subjects
  - Independent assessments of compliance
- If some rules only to apply to ‘significant’ data controllers, establish criteria for defining them such as:
  - Nature of the DFS products or business model.
  - Volume and sensitivity of data that is processed.

- Number of data subjects.
- Turnover.
- Risk of harm to data subjects e.g., on basis of discrimination or bias.
- Use of new technologies for data processing, such as automated processing and profiling.

1.4. GUIDING PRINCIPLE: DEVELOP DP4DFS LEGAL FRAMEWORK

KEY RECOMMENDATIONS:

> Consider regional/international good practices relevant to DP4DFS.

> Apply framework to both public and private entities.

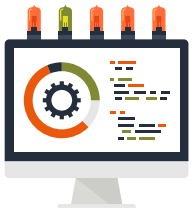
> Establish key definitions and concepts (see suggestions in Annex 3).

> Consider any exceptions that might apply, e.g., for data covered by other laws such as credit reporting or debt collection, for data processing permitted or required by another law or where there are overriding considerations such as national security.

> Provide a transitional period for industry to change processes and procedures and IT systems and to build public awareness.

> Develop public awareness campaign for new DP4DFS framework and related rights and responsibilities.

PILLAR 2: DATA CONTROLLER AND PROCESSOR OBLIGATIONS



This Pillar sets out suggestions for the main obligations to be imposed on data controllers and data processors, including key data processing principles.

2.1 GUIDING PRINCIPLE: REQUIRE EFFECTIVE DP4DFS INTERNAL GOVERNANCE ARRANGEMENTS

KEY RECOMMENDATIONS:

- Require that data controllers:
  - Ensure employees and agents are trained and aware of DP4DFS rules
  - Develop and maintain documented policies and procedures consistent with DP4DFS rules
  - Ensure senior management/Board oversight of compliance with DP4DFS rules
  - Have adequate technological and organizational systems and resources

> Mandate that internal audit function reviews compliance with all DP4DFS rules.

> Require an annual independent assessment of compliance with DP4DFS rules.

2.2 GUIDING PRINCIPLE: ESTABLISH OVERARCHING DATA PROCESSING PRINCIPLES

KEY RECOMMENDATIONS:

> Make foundation implementation of proactive Privacy by Design principles that are set out in a policy, which is approved and monitored by governing body of the relevant entity and published on their website and possibly that of the DPA.[64]

> Set overarching obligation to ensure processing is always (regardless of consent) fair, lawful, and transparent.

> Establish other data processing principles, including:
  - Processing limitation: require processing to be with consent unless it is strictly for purposes of DFS

64 See also World Bank Group. Digital ID and the Data Protection Challenge: Practitioner's Note. 2019

contract or as required or permitted by law
- Data minimization: require that data be limited to purposes of processing
- Accuracy: require data to be accurate and up-to-date and to be corrected or erased if that is not the case
- Storage limitation: require that information be retained only for term consistent with purpose of processing
- Records: require that records of all processing activities be maintained
- Security: require processing to minimize risk of unauthorized or unlawful processing and accidental loss or damage

> Require documented risk- based Privacy Impact Assessments to be conducted on processing activities likely to be high risk to privacy of data subjects, especially considering:
- Use of new technologies
- Nature, scale, and purposes of processing
- Capabilities and needs of data subjects and especially vulnerable groups

> Include specific obligation to ensure processes and related technologies do not result in discriminatory or biased decisions and put burden of proof on data controller/processor to prove there has not been a breach of this obligation.

2.3 GUIDING PRINCIPLE: CREATE MODEL FOR INFORMED AND EFFECTIVE CONSENT

KEY RECOMMENDATIONS:

> Assess local impediments to achieving effective consent, especially considering needs of vulnerable groups (e.g., for verbal consents, use of local languages, access to digital forms of consent and also financial literacy levels)

> Require that all consents:
- Be freely given, informed and unambiguous
- Be in simple and clear terms and as brief as possible
- Be given for specific purposes
- Not be bundled (in particular consent for processing for DFS service should be separated from consent for other purposes)
- Be opt-in rather than opt-out (the default should be opt-out)
- Be separated from other information e.g., terms and conditions
- Be time-limited
- Be able to be withdrawn, with withdrawal being as easy as giving consent
- Be able to be retained for future reference

> Apply same consent rules to all types of data (sensitive or not).

> Make regulations/provide guidelines as to practical meaning of each element of consent rules for DFS, with examples.

> Provide that the data controller or processor has onus of proving consent.

2.4 GUIDING PRINCIPLE: REQUIRE DATA PROTECTION OFFICER WHERE APPROPRIATE

KEY RECOMMENDATIONS:

> Require appointment of appropriately resourced and independent Data Protection Officer, where nature, scope, context, and purposes of processing activities are sufficiently large and/ or significant.

> Specify functions of Data Protection Officer to include e.g.:
- Advice on DP4DFS rules
- Monitor compliance with rules
- Point of contact for data subjects with queries / complaints
- Point of contact for DPA and other regulators
- Facilitate capacity building of staff / agents
- Privacy impact assessments

PILLAR 3: DATA SUBJECT RIGHTS

This Pillar sets the key rights that might be provided to data subjects.

3.1 GUIDING PRINCIPLE: ESTABLISH FUNDAMENTAL RIGHTS OF DATA SUBJECTS

KEY RECOMMENDATIONS:

- Right to information about processing and relevant processors / controllers
- Right of anonymity
- Right to access
- Right to rectification/correction
- Right to erasure/right to be forgotten
- Right to restrict/object to processing
- Right to data portability
- Right not to be subject to a decision based solely on automated processing (e.g., using algorithms and/or machine learning), including profiling other than with express consent or if permitted by law

3.2 GUIDING PRINCIPLE: SPECIFY HOW RIGHTS MAY BE EXERCISED BY DATA SUBJECTS

KEY RECOMMENDATIONS:

- Include provisions explaining how rights may be exercised by data subjects e.g., applicable processes, time limits for responses, templates, appeal rights.

PILLAR 4: CONSUMER AWARENESS AND RECOURSE

This Pillar covers proposals for internal and external complaint and dispute resolution schemes, recourse rights for data subjects and public awareness programs.

4.1 GUIDING PRINCIPLE: REQUIRE EFFECTIVE INTERNAL COMPLAINTS HANDLING PROCEDURES

KEY RECOMMENDATIONS:

- Require data controllers and processors to have documented, transparent, free, and effective procedures for complaints resolution covering e.g., expeditious settlement of complaints; diverse channels to make complaints; and publicity as to complaints processes.

4.2 GUIDING PRINCIPLE: PROVIDE FOR AN EXTERNAL DISPUTE RESOLUTION SCHEME FOR DATA SUBJECTS

KEY RECOMMENDATIONS:

- Provide external body (such as DPA, financial sector supervisor or ombudsman body) (EDR) with power to deal with disputes concerning DP4DFS
- Allow EDR to initiate investigation or court action on behalf of data subjects (including a class) on their own initiative or at the request of data subjects.
- Ensure EDR has power to:
  - make binding decisions
  - award compensation
  - order correction of data
- Require EDR to publicize decisions in relation to disputes.

4.4 GUIDING PRINCIPLE: CONSIDER NEED FOR PUBLIC AWARENESS PROGRAMS

KEY RECOMMENDATIONS:

- Encourage DFS providers to promote awareness of data privacy issues including data subject rights and key risks (e.g., as to identify theft and fraud).
- Consider development of a specific public awareness campaign to cover rights and responsibilities under new DP4DFS framework.
- Take data privacy issues and specific needs of vulnerable groups into account in financial literacy programs.

PILLAR 5: SUPERVISION AND ENFORCEMENT

This Pillar covers a range of important issues relevant to supervision and enforcement including risk-based supervision; supervisory mandate, powers, capacity and resources; the need for consultation and coordination on an ongoing basis; establishing a credible threat of enforcement and considering data privacy in a regulatory sandbox environment.

5.1 GUIDING PRINCIPLE: TAKE A RISK-BASED AND PROPORTIONATE APPROACH TO SUPERVISION

KEY RECOMMENDATIONS:

- Supervise DP4DFS rules on a firm and market risk basis.
- Develop a methodology for assessing privacy risks in DFS business models from e.g., information sources, information sensitivity, use cases and systems interconnectivity.

5.2 GUIDING PRINCIPLE: ENSURE SUPERVISORS HAVE EFFECTIVE MANDATE, POWERS, CAPACITY, AND RESOURCES

KEY RECOMMENDATIONS:

- Provide supervisors with clear DP4DFS mandate.
- Ensure appropriate powers for supervisor e.g., to supervise, to assess use of FinTech-related technologies or require evidence of how they are used; to issue fines, to grant exemptions, to make orders to ban/suspend DFS processing practices, to register or de-register data controllers and to handle complaints.
- Ensure supervisor has organizational and technological capacity and resources to design, implement and supervise DP4DFS now and in future, taking into account likely FinTech developments.
- Consider current environment and likely future developments. e.g., open banking.

5.3 GUIDING PRINCIPLE: ESTABLISH CLEAR CONSULTATION AND COORDINATION FRAMEWORK

KEY RECOMMENDATIONS:

- Provide for ongoing consultation and coordination with public sector stakeholders on policy and regulatory issues, FinTech innovations and systemic DP4DFS issues.
- Implement consultation mechanism with DFS industry and civil society groups (e.g., privacy advocates and consumer associations).
- Consider if Industry Advisory Group is desirable.[65]
- Establish MOUs with key regulators and government agencies.
- Consider regional data privacy initiatives.

5.4 GUIDING PRINCIPLE: CONSIDER DP4DFS ISSUES IN REGULATORY SANDBOX ENVIRONMENTS

KEY RECOMMENDATIONS:

- Consider data privacy issues when testing DFS innovations in regulatory sandboxes.
- Consider thematic regulatory sandboxes specifically for DP4DFS innovations.

5.5 GUIDING PRINCIPLE: ENSURE CREDIBLE THREAT OF ENFORCEMENT

KEY RECOMMENDATIONS:

- Ensure sanctions are significant enough to be effective.
- Publicize all enforcement action.
- Require notice of significant breaches to regulators/ and data subjects.
- Consider making provision for fines to be a percentage of profits or turnover and/or a specified flat amount.
- Consider basing fines on severity of breaches.

65 See, for example, Personal Data Protection Advisory Committee in Malaysia

PILLAR 6: DP4DFS IN GLOBAL AND NATIONAL EMERGENCIES

This Pillar contains recommendations for dealing with DP4DFS issues in an emergency, such as COVID-19 but also applying more generally.

6.1 GUIDING PRINCIPLE: PROVIDE POLICY GUIDANCE ON APPLICATION OF DP4DFS IN EMERGENCIES

KEY RECOMMENDATIONS:

- Consider regulatory guidance for data controllers/ processors on specific data privacy challenges and expectations.
- Ensure consultation between data privacy and financial sector regulatory authorities.
- Consider DP4DFS challenges in any national coordinating body.

6.2 GUIDING PRINCIPLE: ENSURE DP4DFS LEGAL FRAMEWORK MAKES PROVISION FOR EMERGENCIES

KEY RECOMMENDATIONS:

- Consider powers to provide relief from DP4DFS rules in an emergency.
- If power does not currently exist consider amendment to law.

6.3 GUIDING PRINCIPLE: EXERCISE APPROPRIATE FLEXIBILITY AS TO ENFORCEMENT IN APPROPRIATE CASES

KEY RECOMMENDATIONS:

- Consider providing regulatory relief from existing data privacy and identity laws for the purposes of the emergency to both public and private sector entities.
- Ensure any relief provided is:
  - Proportionate as to risks
  - Clear
  - Transparent to the public
  - Specific as to purposes
  - Time – limited to period of crisis
- Make clear accountability of regulatory authorities providing relief.
- Prohibit sharing of data with third parties except to the extent specifically permitted.
- Encourage industry to engage with government and data privacy and financial sector supervisory authorities on DP4DFS issues.

MINIMALIST DP4DS APPROACH FOR FINANCIAL SECTOR REGULATORS

This proposal contains suggestions as to the minimal actions that financial sector regulators might take in the interim period before there is a comprehensive data protection law in place.

1. CONDUCT HIGH-LEVEL ASSESSMENT OF THE DFS MARKET AND RELATED DATA PRIVACY RISKS

- Cover both public and private sectors, including products, providers (traditional and FinTech based), delivery channels, customer segments, types of data used and analytic tools.
- Develop methodology for assessing privacy risks in DFS business models from e.g., information sources, information sensitivity, use cases and systems interconnectivity.
- Consider especially, the needs of vulnerable groups.
- Consider financial inclusion objectives.

2. ESTABLISH CONSULTATION MECHANISM FOR NEW DP4DFS RULES

Include public, private, and civil society representatives and ensure both traditional and FinTech entities are consulted.

3. ESTABLISH RISK-BASED CRITERIA FOR DEFINING 'SIGNIFICANT' DFS DATA CONTROLLERS

Such criteria could cover, e.g.:

- Volume and sensitivity of data processed
- Number of data subjects
- Turnover
- Risk of harm to data subjects e.g., on basis of discrimination or bias
- Use of new technologies for data processing, such as automated processing and profiling

4. DEVELOP NEW DP4DFS RULES

Risk-based priority rules could cover:

- Privacy by design and default governance and resource arrangements
- Transparent information for data subjects about data processing
- Effective and informed consents
- Rights to access and correction, and to object to processing
- Recourse for data subjects with complaints (e.g., as to compensation or data correction)

5. CONSIDER ALSO RULES FOR 'SIGNIFICANT' DATA CONTROLLERS AND PROCESSORS

Rules could cover, e.g., needs for registration; Data Privacy Officer; privacy impact Assessments; breach reporting to regulators and to data subjects; and independent assessments of compliance.

6. BUILD CONSUMER AWARENESS OF DP4DFS

Have specific focus on the diverse needs of vulnerable groups, education on data privacy risks with DFS, and related rights and responsibilities.

7. MAINTAIN ONGOING CONSULTATION ARRANGEMENTS WITH KEY STAKEHOLDERS

For example: key ministries and regulators, FinTech and traditional DFS data controllers and consumer associations.

ABBREVIATIONS AND ACRONYMS

ACRO rights	Access, recertification, cancellation, and objection rights
AFI	Alliance for Financial Inclusion
AML/CFT	Anti-Money Laundering and Counter-Terrorism Financing
BTCA	Better Than Cash Alliance
CEMCWG	Consumer Protection and Market Conduct Working Group
CFI	Centre for Financial Inclusion
CGAP	Consultative Group to Assist the Poor
DP	Data Privacy
DPA	Data Privacy Authority
DP4DFS	Data Privacy for Digital Financial Services
DFS	Digital Financial Services
DFSWG	Digital Financial Services Working Group
DPO	Data Privacy Officer
G2P	Government to Person
GDPR / General Data Protection Regulation	EU Regulation 2016/79 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data
OECD	Organisation for Economic Co-operation and Development
PSD2	EU Directive 2015/2366 on Payments Services in the Internal Market
WB	World Bank Group

ANNEX 1.
LIST OF ORGANIZATIONS INTERVIEWED FOR THE PROJECT

COUNTRY / REGION	ORGANIZATION	NAME	POSITION
GLOBAL	CFI	Mayada El Zohghbi	Managing Director
		Alexandra Rizzi	Senior Director and Data Privacy Lead
GLOBAL	CRIF	Davide M. Meo	International Markets Director
		Valeria Racemoli	Senior Regulatory Specialist
GLOBAL	CGAP	David Medine	Consultant
GLOBAL	CGAP	Ivo Jenik	Financial Sector Specialist
GLOBAL	GSMA	Brian Muthiora	Regulatory Director, Africa
GLOBAL	Vodacom	Judith Obholzer	Managing Executive Public Policy
		Mpumi Simelane	Group Privacy Officer
GLOBAL	Home Credit	Lucas Frohlich	Senior Legal Manager
		Vit Papousek	External Affairs Manager
AUSTRALIA	University of New South Wales	Dr Katherine Kemp	Senior Lecturer Faculty of Law
GHANA	Data Protection Commission	Patricia Adusei-Poku	Executive Director / Commissioner Data Protection Commission
PHILIPPINES	Data Protection Commission	Ivy Grace Villasoto and others	Director, Privacy Policy Office
	Bangko Sentral ng Pilipinas	Ellen Joyce Suficiencia and others	Director, Center for Learning Inclusion and Strategy

ANNEX 2.
KEY REGULATORY FRAMEWORKS ANALYSED

COUNTRY	KEY REGULATORY FRAMEWORKS
AUSTRALIA	Privacy Act (1988)
BRAZIL	Personal Data Protection Law (2018)
EU	General Data Protection Regulation (2016)
GHANA	Data Protection Act (2012)
INDIA	Draft Personal Data Protection Bill (2019) RBI Non - Banking Financial Company Account Aggregator Master Direction (2016) (updated to November 22, 2019)
KENYA	Data Protection Act (2019)
MALAYSIA	Personal Data Protection Act (2010) Personal Data Protection Code of Practice for the Banking and Financial Sector (2017)
MEXICO	Federal Law on Protection of Personal Data held by Private Persons (2010) and Regulations (2012)
PERU	Personal Data Protection Law (2011) and Regulations (2013)
PHILIPPINES	Data Privacy Act (2012) and Implementing Rules and Regulations NPC Circular No. 20-01 Guidelines on the Processing of Personal Data for Loan – Related Transactions (2020)
SOUTH AFRICA	Protection of Personal Information Act (2013)

ANNEX 3.
KEY CONCEPTS AND DEFINITIONS

CONCEPT	DEFINITION
CONTROLLER	A natural or legal entity or public authority, which alone or jointly with others, determines the purpose or method of processing personal data.
DATA SUBJECT	An individual whose personal data is or may be processed.
FINTECH	The application of technology in finance (in brief, 'Financial Technology').[66]
ID	An official means of identification of an individual.
OPEN BANKING	Data sharing schemes based on customer consent where data is shared by financial institutions with third parties (such as other financial institutions, payments service providers, data aggregators, and commercial partners).
PERSONAL DATA	Any information or an opinion relating to an identified or identifiable individual, whether true or not and whether kept in a material form or not and whether automated or not.
PROCESSOR	A natural or legal entity or public authority, which processes personal data on behalf of the controller.
PROCESSING	Any operation conducted in relation to personal data whether manually or automatically including collection, use, disclosure, storage, recording, erasure, or otherwise and 'processes', 'processed' and similar words have a similar meaning, but excluding any processing: • required for the purposes of specified activities (such as a judicial function, enforcement of a claim, national security or a purely domestic or household purpose); or • undertaken for a purpose required or permitted by law.
PROFILING	A form of processing that analyses, evaluates, or predicts personal aspects relevant to an individual, including (without limitation) their behavior, attributes, preferences, or characteristics.
SENSITIVE INFORMATION	Information or an opinion about a person's financial data, biometric data, official identifier, religious, political, or philosophical beliefs or affiliation, union membership, race, ethnicity, caste, health and sexual identity.
VULNERABLE GROUPS	Individuals who may be especially vulnerable in the context of DP4DFS, such as women, youth, the elderly, persons with disabilities and displaced persons.

66 Bank for International Settlements (BIS) Basel Committee on Banking Supervision: Report on Open Banking and Application Programming Interfaces (2019) (Footnotes 1 and 2)

ANNEX 4. INTERNATIONAL GOOD PRACTICES FOR DP4DFS

International organizations have developed guidance on good practices relevant to DP4DFS.

Examples include:

- **The World Bank:** Good Practices for Financial Consumer Protection (2017) (see Annex A, section D)
- **Better Than Cash Alliance:** Responsible Digital Payments Guidelines (2016) (see Guideline 7)
- **G20:** High-Level Principles for Digital Financial Inclusion (2016) (see Principles 2 and 5)
- **GSMA:** Guidelines on Mobile Money Data Protection (2018). See also GSMA: Data Protection in Mobile Money (2019) and GSMA: Smart Data Privacy Laws. Achieving the Right Outcomes for the Digital Age (2019)
- **OECD (2020):** Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-Centric Analysis (2020)

ANNEX 5. REFERENCES

AFI KNOWLEDGE PRODUCTS

AFI: Special Report on Creating Enabling FinTech Ecosystems: The Role of Regulators (2020) https://www.afi-global.org/publications/3181/Creating-Enabling-FinTech-Ecosystems-The-Role-of-Regulators

AFI: Policy Framework for Leveraging Digital Financial Services to respond to Global Emergencies – Case of COVID-19 (2020) https://www.afi-global.org/sites/default/files/publications/2020-10/AFI_DFSWG_COVID_PF_AW4_digital.pdf

AFI: Policy Model on Consumer Protection for Digital Financial Services (2020) https://www.afi-global.org/publications/3465/Policy-Model-on-Consumer-Protection-for-Digital-Financial-Services

AFI: Policy Framework for Responsible Digital Credit (2020) https://www.afi-global.org/publications/3216/Policy-Framework-for-Responsible-Digital-Credit

AFI: Policy Model for E-Money (2019) https://www.afi-global.org/publications/3088/Policy-Model-for-E-Money

AFI: KYC Innovations, Financial Inclusion and Integrity In Selected AFI Member Countries (2019) https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries.pdf

AFI: Special Report on FinTech for Financial Inclusion: A Framework for Digital Financial Transformation (2018) https://www.afi-global.org/publications/2844/FinTech-for-Financial-Inclusion-A-Framework-for-Digital-Financial-Transformation

Global Data Bases of Data Privacy and Protection Laws DLA Piper Data Protection Laws of the World https://www.dlapiperdataprotection.com/

UNCTAD Data Protection and Privacy Legislation Worldwide https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

OTHER PUBLICATIONS

Arner DW, Buckley RP, Zetzsche, DA and Veidt, R: Sustainability, FinTech and Financial Inclusion Eur Bus Org Law Rev 21, 7–35 (2020) https://doi.org/10.1007/s40804-020-00183-y

Australia: Attorney – General's Department: Privacy Act Review Issues Paper (2020) https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper

Bank for International Settlements (BIS) Basel Committee on Banking Supervision: Report on Open Banking and Application Programming Interfaces (2019) https://www.bis.org/bcbs/publ/d486.htm

Better Than Cash Alliance: Responsible Digital Payments Guidelines (2016) https://www.betterthancash.org/tools-research/case-studies/responsible-digital-payments-guidelines

Carpenter v. United States 585 U.S. ___ (2018) https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

Centre for Financial Inclusion (CFI) and Institute of International Finance: Accelerating Financial Inclusion with New Data (2018) https://www.centerforfinancialinclusion.org/accelerating-financial-inclusion-with-new-data-2

CFI: Blog - Data Protection and Financial Inclusion: Why It Matters (Introduction) (2020)https://www.centerforfinancialinclusion.org/data-protection-and-financial-inclusion-why-it-matters-introduction

CFI: Blog - Data Consent: Let's Share the Burden for Effective Consumer Protection (2020)https://www.centerforfinancialinclusion.org/data-consent-lets-share-the-burden-for-effective-consumer-protection

CFI: Blog - Data for Inclusive Finance: Delivering on the Promise for Consumers (2020)https://www.centerforfinancialinclusion.org/data-for-inclusive-finance-delivering-on-the-promise-for-consumers

CGAP: Blog - A Growing Trend in Financial Regulation: Thematic Sandboxes (2019)https://www.cgap.org/blog/growing-trend-financial-regulation-thematic-sandboxes

CGAP: Focus Note - Is Data Privacy Good for Business? (2019)https://www.cgap.org/sites/default/files/publications/2019_12_Focus_Note_Is_Data_Privacy_Good_for_Business.pdf

CGAP: Making Data Work for the Poor: New Approaches to Data Protection and Privacy (2020)https://www.cgap.org/research/publication/making-data-work-poor

CGAP: Blog - Open Banking: 7 Ways Data-Sharing Can advance Financial inclusion (2020)https://www.cgap.org/blog/open-banking-7-ways-data-sharing-can-advance-financial-inclusion

CGAP: Blog - Blog Data Privacy Concerns Influence Financial Behaviors in India, Kenya (2020)https://www.cgap.org/blog/data-privacy-concerns-influence-financial-behaviors-india-kenya

CGAP: Blog – Open Data and the Future of Banking (2019)https://www.cgap.org/blog/open-data-and-future-banking

Centre for Information Policy Leadership: Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice (2019) https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/07/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf

Covington and Burlington LLP: Overlap between the GDPR and PSD2 Inside Privacy (2018) https://www.insideprivacy.com/financial-institutions/overlap-between-the-gdpr-and-psd2/

Deloitte: After the dust settles. How Financial Services are taking a Sustainable Approach to GDPR Compliance in a New Era for Privacy, one year on https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-the-impact-of-gdpr-on-the-financial-services.pdf

European Data Protection Supervisor: The EDPS quick guide to necessity and proportionality (2020) https://edps.europa.eu/data-protection/our-work/publications/factsheets/edps-quick-guide-necessity-and-proportionality_en

European Parliament: Parliamentary Questions: Question Reference: E-000054/2019 (10 March 2019) https://www.europarl.europa.eu/doceo/document/E-8-2019-000054-ASW_EN.html

Kemp K, University of New South Wales: Big Data, Financial Inclusion and Privacy for the Poor. Responsible Finance Forum (2017) https://responsiblefinanceforum.org/big-data-financial-inclusion-privacy-poor/

Kemp K; Buckley RP, 'Protecting Financial Consumer Data in Developing Countries: An Alternative to the Flawed Consent Model, Georgetown Journal of International Affairs, vol. 18, pp. 35 – 46 (2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3237856

Finextra: Blog by Carlo R.W. de Meijer Economist and Researcher at De Meijer Independent Financial Services Advisory (MIFSA): Blockchain versus GDPR and who should adjust most (2018) https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most

G20: High-Level Principles for Digital Financial Inclusion (2016) https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion

G20/OECD Policy Guidance: Financial Consumer Protection Approaches: Financial Consumer Protection in the Digital Age (2018) https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf

GSMA: The Impact of Data Localisation Requirements on the Growth of Mobile Money – Enabled Remittances (2018) https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf

GSMA: Guidelines on Mobile Money Data Protection (2018) https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/09/GSMA-Guidelines-on-mobile-money-data-protection.pdf

GSMA: Data Protection in Mobile Money (2019) https://www.gsma.com/mobilefordevelopment/resources/data-protection-in-mobile-money/

GSMA: Smart Data Privacy Laws. Achieving the Right Outcomes for the Digital Age (2019) https://www.gsma.com/publicpolicy/wp-content/uploads/2019/06/GSMA_Smart-Data-Privacy-Laws_Report_June-2019.pdf

GSMA: State of the Industry Report on Mobile Money (2019) https://www.gsma.com/sotir/wp-content/uploads/2020/03/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2019-Full-Report.pdf

GSMA: State of Mobile Internet Connectivity Report (2020) https://www.gsma.com/r/wp-content/uploads/2020/09/GSMA-State-of-Mobile-Internet-Connectivity-Report-2020.pdf

GSMA: The GSMA COVID-19 Privacy Guidelines (2020) https://www.gsma.com/publicpolicy/resources/covid-19-privacy-guidelines

International Monetary Fund (IMF): The Promise of FinTech Financial Inclusion in the Post COVID-19 Era. No. 20/09 (2020) https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2020/06/29/The-Promise-of-Fintech-Financial-Inclusion-in-the-Post-COVID-19-Era-48623

IMF: Special Series on COVID-19 - Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies (2020)

International Telecommunication Union (ITU): Focus Group on Digital Financial Services, Focus Group Report on Commonly Identified Consumer Protection Themes for Digital Financial Services 05/2016 (2016) https://www.itu.int/en/ITUT/focusgroups/dfs/Documents/09_2016/ConsumerProtectionThemesForBestPractices.pdf

ITU: Financial Inclusion Global Initiative (FIGI) Security Infrastructure and Trust Working Group, Big data, machine learning, consumer protection and privacy (2018) https://www.itu.int/en/ITU-T/extcoop/figisymposium/2019/Documents/Presentations/Big%20data,%20Machine%20learning,%20Consumer%20protection%20and%20Privacy.pdf

McDonald AM and Cranor LF: The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568 (2008) https://kb.osu.edu/handle/1811/72839

OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980, updated in 2013) http://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OECD: Ensuring Data Privacy as we battle COVID-19 (2020) https://read.oecd-ilibrary.org/view/?ref=128_128758-vfx2g82fn3&title=Ensuring-data-privacy-as-we-battle-COVID-19

OECD: Personal Data Use in Financial Services and the Role of Financial Education: A Consumer-Centric Analysis (2020) http://www.oecd.org/financial/education/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf

Toronto Centre: Cloud Computing: Issues for Supervisors (2020) https://res.torontocentre.org/guidedocs/Cloud%20Computing%20FINAL.pdf

World Bank: Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting (2018) https://openknowledge.worldbank.org/handle/10986/31009

World Bank: Good Practices for Financial Consumer Protection (2017) https://www.worldbank.org/en/topic/financialinclusion/brief/2017-good-practices-for-financial-consumer-protection

World Bank: Digital ID and the Data Protection Challenge: Practitioner's Note (2019) https://openknowledge.worldbank.org/handle/10986/32629

World Bank: Disruptive Technologies in the Credit Information Sharing Industry: Developments and Implications (2019) http://documents1.worldbank.org/curated/en/587611557814694439/pdf/Disruptive-Technologies-in-the-Credit-Information-Sharing-Industry-Developments-and-Implications.pdf

United Nations (UN): Personal Data Protection and Privacy Principles (2018) https://unsceb.org/sites/default/files/UN-Principles-on-Personal-Data-Protection-Privacy-2018.pdf

Zetzsche, DA, Arner, DW. and Buckley, RP and Kaiser-Yücel, A: FinTech Toolkit: Smart Regulatory and Market Approaches to Financial Technology Innovation (May 2020). University of Hong Kong Faculty of Law Research Paper No. 2020/027 https://ssrn.com/abstract=3598142

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org
Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork